NIST 800-53

[AC - Controles de Acesso 9](#_Toc17904332)

[AC-1: Política e Procedimentos de Controle de Acesso (P1) 9](#_Toc17904333)

[AC-2: Gestão de Conta (P1) 9](#_Toc17904334)

[AC-3: Garantia de Acesso (P1) 14](#_Toc17904335)

[AC-4: Aplicação do Fluxo de Informação (P1) 17](#_Toc17904336)

[AC-5: Segregação de Funções (P1) 23](#_Toc17904337)

[AC-6: Menor Privilégio (P1) 23](#_Toc17904338)

[AC-7: Tentativas de Login Incorretas (P2) 26](#_Toc17904339)

[AC-8: Notificação de Utilização do Sistema (P1) 27](#_Toc17904340)

[AC-9: Notificação de Login Anterior (Acesso) (P0) 28](#_Toc17904341)

[AC-10: Controle de Sessões Simultâneas (P3) 28](#_Toc17904342)

[AC-11: Bloqueio da Sessão (P3) 29](#_Toc17904343)

[AC-12: Encerramento da Sessão (P2) 29](#_Toc17904344)

[AC-13: Supervisão e Revisão - Controle de Acesso (P0) 30](#_Toc17904345)

[AC-14: Ações Permitidas Sem Identificação ou Autenticação (P3) 30](#_Toc17904346)

[AC-15: Marcação Automatizada (P0) 31](#_Toc17904347)

[AC-16: Atributos de Segurança (P0) 31](#_Toc17904348)

[AC-17: Acesso Remoto (P1) 34](#_Toc17904349)

[AC-18: Acesso Sem Fio (P1) 37](#_Toc17904350)

[AC-19: Controle de Acesso para Dispositivos Móveis (P1) 38](#_Toc17904351)

[AC-20: Utilização de Sistemas Externos (P1) 40](#_Toc17904352)

[AC-21: Compartilhamento de Informações (P2) 42](#_Toc17904353)

[AC-22: Conteúdo Público Acessível (P3) 43](#_Toc17904354)

[AC-23: Proteção contra Mineração de Dados (P0) 43](#_Toc17904355)

[AC-24: Decisões sobre Controle de Acesso (P0) 44](#_Toc17904356)

[AC-25: Monitor de Referência (P0) 45](#_Toc17904357)

[AU - Auditoria e Responsabilidade 46](#_Toc17904358)

[AU-1: Política e Procedimentos de Auditoria e Responsabilidade (P1) 46](#_Toc17904359)

[AU-2: Eventos de Auditoria (P1) 46](#_Toc17904360)

[AU-3: Conteúdo dos Registros de Auditoria (P1) 48](#_Toc17904361)

[AU-4: Capacidade do Armazenamento de Auditoria (P1) 49](#_Toc17904362)

[AU-5: Resposta a Falhas de Processamento de Auditoria (P1) 49](#_Toc17904363)

[AU-6: Revisão, Análise e Relatório de Auditoria (P1) 51](#_Toc17904364)

[AU-7: Resumo da Auditoria e Geração de Relatório (P2) 53](#_Toc17904365)

[AU-8: Marcação de Tempo (P1) 54](#_Toc17904366)

[AU-9: Proteção das Informações de Auditoria (P1) 55](#_Toc17904367)

[AU-10: Não-Repúdio (P2) 56](#_Toc17904368)

[AU-11: Retenção dos Dados de Auditoria (P3) 58](#_Toc17904369)

[AU-12: Geração de Auditoria (P1) 59](#_Toc17904370)

[AU-13: Monitoramento da Divulgação de Informações (P0) 60](#_Toc17904371)

[AU-14: Auditoria da Sessão (P0) 60](#_Toc17904372)

[AU-15: Capacidade de Auditoria Alternativa (P0) 61](#_Toc17904373)

[AU-16: Auditoria Organizacional Transversal (P0) 61](#_Toc17904374)

[AT - Conscientização e Treinamento 63](#_Toc17904375)

[AT-1: Política e Procedimentos de Conscientização e Formação em Segurança (P1) 63](#_Toc17904376)

[AT-2: Treinamento de Conscientização em Segurança (P1) 64](#_Toc17904377)

[AT-3: Treinamento de Segurança Baseado em Cargo (P1) 65](#_Toc17904378)

[AT-4: Registros de Treinamento de Segurança (P3) 67](#_Toc17904379)

[AT-5: Contatos com Grupos de Segurança e Associações (P0) 67](#_Toc17904380)

[CM - Gestão de Configurações 68](#_Toc17904381)

[CM-1: Política e Procedimentos de Gestão da Configuração (P1) 68](#_Toc17904382)

[CM-2: Configuração Base de Referência (P1) 68](#_Toc17904383)

[CM-3: Controle sobre Alterações de Configuração (P1) 71](#_Toc17904384)

[CM-4: Análise de Impacto de Segurança (P2) 73](#_Toc17904385)

[CM-5: Restrições de Acesso para Mudanças (P1) 74](#_Toc17904386)

[CM-6: Definições de Configuração (P1) 76](#_Toc17904387)

[CM-7: Menor Funcionalidade (P1) 78](#_Toc17904388)

[CM-8: Inventário de Componentes do Sistema (P1) 80](#_Toc17904389)

[CM-9: Plano de Gerenciamento de Configuração (P1) 83](#_Toc17904390)

[CM-10: Restrições de Uso do Software (P2) 84](#_Toc17904391)

[CM-11: Software Instalado pelo Usuário (P1) 84](#_Toc17904392)

[CP - Planejamento de Contingência 86](#_Toc17904393)

[CP-1: Política e Procedimentos do Planeamento de Contingência (P1) 86](#_Toc17904394)

[CP-2: Plano de Contingência (P1) 87](#_Toc17904395)

[CP-3: Treinamento de Contingência (P2) 90](#_Toc17904396)

[CP-4: Teste do Plano de Contingência (P2) 91](#_Toc17904397)

[CP-5: Atualização do Plano de Contingência (P0) 92](#_Toc17904398)

[CP-6: Local de Armazenamento Alternativo (P1) 92](#_Toc17904399)

[CP-7: Local de Processamento Alternativo (P1) 94](#_Toc17904400)

[CP-8: Serviços de Telecomunicações (P1) 95](#_Toc17904401)

[CP-9: Backup do Sistema (P1) 97](#_Toc17904402)

[CP-10: Recuperação e Reconstituição do Sistema (P1) 99](#_Toc17904403)

[CP-11: Protocolos de Comunicação Alternativa (P0) 100](#_Toc17904404)

[CP-12: Modo de Segurança (P0) 100](#_Toc17904405)

[CP-13: Mecanismos de Segurança Alternativos (P0) 101](#_Toc17904406)

[IA - Identificação e Autenticação 102](#_Toc17904407)

[IA-1: Política e Procedimentos de Identificação e Autenticação (P1) 102](#_Toc17904408)

[IA-2: Identificação e Autenticação (Usuários Organizacionais) (P1) 103](#_Toc17904409)

[IA-3: Identificação e Autenticação do Dispositivo (P1) 107](#_Toc17904410)

[IA-4: Gestão do Identificador (P1) 108](#_Toc17904411)

[IA-5: Gestão do Autenticador (P1) 110](#_Toc17904412)

[IA-6: Feedback do Autenticador (P2) 115](#_Toc17904413)

[IA-7: Autenticação de Módulo Criptográfico (P1) 115](#_Toc17904414)

[IA-8: Identificação e Autenticação (Usuários Não Organizacionais) (P1) 116](#_Toc17904415)

[IA-9: Identificação e Autenticação de Serviços (P0) 118](#_Toc17904416)

[IA-10: Identificação Adaptativa e Autenticação (P0) 119](#_Toc17904417)

[IA-11: Re-Autenticação (P0) 119](#_Toc17904418)

[IR - Resposta a Incidentes 121](#_Toc17904419)

[IR-1: Política e Procedimentos de Resposta a Incidentes (P1) 121](#_Toc17904420)

[IR-2: Treinamento de Resposta a Incidentes (P2) 122](#_Toc17904421)

[IR-3: Teste de Resposta a Incidentes (P2) 122](#_Toc17904422)

[IR-4: Manuseio de Incidentes (P1) 123](#_Toc17904423)

[IR-5: Monitoramento de Incidentes (P1) 126](#_Toc17904424)

[IR-6: Relatórios de Incidentes (P1) 127](#_Toc17904425)

[IR-7: Assistência à Resposta a Incidentes (P2) 128](#_Toc17904426)

[IR-8: Plano de Resposta a Incidentes (P1) 129](#_Toc17904427)

[IR-9: Resposta ao Vazamento de Informação (P0) 130](#_Toc17904428)

[IR-10: Equipe Integrada de Análise da Segurança da Informação (P0) 131](#_Toc17904429)

[MA - Manutenção 132](#_Toc17904430)

[MA-1: Política e Procedimentos da Manutenção de Sistemas (P1) 132](#_Toc17904431)

[MA-2: Manutenção Controlada (P2) 132](#_Toc17904432)

[MA-3: Ferramentas de Manutenção (P3) 134](#_Toc17904433)

[MA-4: Manutenção Não Local (P2) 135](#_Toc17904434)

[MA-5: Manutenção Pessoal (P2) 137](#_Toc17904435)

[MA-6: Manutenção Programada (P2) 139](#_Toc17904436)

[MP - Proteção de Mídia 141](#_Toc17904437)

[MP-1: Política e Procedimentos de Proteção de Mídia (P1) 141](#_Toc17904438)

[MP-2: Acesso à Mídia (P1) 141](#_Toc17904439)

[MP-3: Marcação de Mídia (P2) 142](#_Toc17904440)

[MP-4: Armazenamento de Mídia (P1) 143](#_Toc17904441)

[MP-5: Transporte de Mídia (P1) 144](#_Toc17904442)

[MP-6: Sanitização de Mídia (P1) 145](#_Toc17904443)

[MP-7: Uso de Mídia (P1) 148](#_Toc17904444)

[MP-8: Descarte de Mídia (P0) 149](#_Toc17904445)

[PS - Segurança Pessoal 151](#_Toc17904446)

[PS-1: Política e Procedimentos de Segurança dos Funcionários (P1) 151](#_Toc17904447)

[PS-2: Designação de Riscos de Cargo (P1) 151](#_Toc17904448)

[PS-3: Entrevista de Funcionários (P1) 152](#_Toc17904449)

[PS-4: Desligamento de Funcionários (P1) 153](#_Toc17904450)

[PS-5: Transferência de Funcionários (P2) 155](#_Toc17904451)

[PS-6: Acordos de Acesso (P3) 155](#_Toc17904452)

[PS-7: Segurança dos Terceiros (P1) 157](#_Toc17904453)

[PS-8: Sanções dos Funcionários (P3) 157](#_Toc17904454)

[PE - Proteção Física e Ambiental 159](#_Toc17904455)

[PE-1: Política e Procedimentos de Proteção Física e Ambiental (P1) 159](#_Toc17904456)

[PE-2: Autorizações de Acesso Físico (P1) 159](#_Toc17904457)

[PE-3: Controle de Acesso Físico (P1) 161](#_Toc17904458)

[PE-4: Controle de Acesso para Meios de Transmissão (P1) 163](#_Toc17904459)

[PE-5: Controle de Acesso para Dispositivos de Saída (P2) 164](#_Toc17904460)

[PE-6: Monitorando o Acesso Físico (P1) 164](#_Toc17904461)

[PE-7: Controle do Visitante (P0) 166](#_Toc17904462)

[PE-8: Registros de Acesso ao Visitante (P3) 166](#_Toc17904463)

[PE-9: Equipamentos de Energia e Cabos (P1) 166](#_Toc17904464)

[PE-10: Desligamento de Emergência (P1) 167](#_Toc17904465)

[PE-11: Energia de Emergência (P1) 167](#_Toc17904466)

[PE-12: Luz de Emergência (P1) 168](#_Toc17904467)

[PE-13: Proteção Contra Fogo (P1) 168](#_Toc17904468)

[PE-14: Controles de Temperatura e Umidade (P1) 169](#_Toc17904469)

[PE-15: Proteção de Danos a Água (P1) 170](#_Toc17904470)

[PE-16: Entrega e Remoção (P2) 170](#_Toc17904471)

[PE-17: Local de Trabalho Alternativo (P2) 171](#_Toc17904472)

[PE-18: Localização dos Componentes do Sistema de Informação (P3) 171](#_Toc17904473)

[PE-19: Vazamento de Informação (P0) 172](#_Toc17904474)

[PE-20: Monitoramento e Acompanhamento de Ativos (P0) 172](#_Toc17904475)

[PL - Planejamento 174](#_Toc17904476)

[PL-1: Política e Procedimentos do Planejamento de Segurança (P1) 174](#_Toc17904477)

[PL-2: Plano de Segurança do Sistema (P1) 175](#_Toc17904478)

[PL-3: Atualização do Plano de Segurança do Sistema (P0) 176](#_Toc17904479)

[PL-4: Regras de Comportamento (P2) 177](#_Toc17904480)

[PL-5: Avaliação de Impacto de Privacidade (P0) 178](#_Toc17904481)

[PL-6: Planejamento de Atividades Relacionadas com a Segurança (P0) 178](#_Toc17904482)

[PL-7: Conceito de Segurança das Operações (P0) 178](#_Toc17904483)

[PL-8: Arquitetura de Segurança da Informação (P1) 178](#_Toc17904484)

[PL-9: Gestão Central (P0) 180](#_Toc17904485)

[PM - Gestão de Programas 182](#_Toc17904486)

[PM-1: Plano do Programa de Segurança da Informação (P0) 182](#_Toc17904487)

[PM-2: Diretor de Segurança de Informação Sênior (P0) 183](#_Toc17904488)

[PM-3: Recursos de Segurança da Informação (P0) 183](#_Toc17904489)

[PM-4: Plano de Ação e Marcos do Processo (P0) 184](#_Toc17904490)

[PM-5: Inventário do Sistema de Informação (P0) 184](#_Toc17904491)

[PM-6: Medidas de Desempenho da Segurança da Informação (P0) 185](#_Toc17904492)

[PM-7: Arquitetura Empresarial (P0) 185](#_Toc17904493)

[PM-8: Plano de Infraestrutura Crítica (P0) 186](#_Toc17904494)

[PM-9: Estratégia de Gestão de Riscos (P0) 186](#_Toc17904495)

[PM-10: Processo de Autorização de Segurança (P0) 187](#_Toc17904496)

[PM-11: Definição do Processo da Missão/Negócio (P0) 188](#_Toc17904497)

[PM-12: Programa de Ameaças Internas (Insiders) (P0) 188](#_Toc17904498)

[PM-13: Força de Trabalho de Segurança da Informação (P0) 189](#_Toc17904499)

[PM-14: Teste, Treinamento e Monitoramento (P0) 190](#_Toc17904500)

[PM-15: Contatos com Grupos de Segurança e Associações (P0) 191](#_Toc17904501)

[PM-16: Programa de Conscientização sobre Ameaças (P0) 191](#_Toc17904502)

[RA - Avaliação de Riscos 192](#_Toc17904503)

[RA-1: Política e Procedimentos de Avaliação de Riscos (P1) 192](#_Toc17904504)

[RA-2: Categorização de Segurança (P1) 193](#_Toc17904505)

[RA-3: Avaliação de Risco (P1) 193](#_Toc17904506)

[RA-4: Atualização de Avaliação de Riscos (P0) 195](#_Toc17904507)

[RA-5: Digitalização de Vulnerabilidade (P1) 195](#_Toc17904508)

[RA-6: Inquérito à Vigilância Técnica (P0) 197](#_Toc17904509)

[CA - Avaliação e Autorização de Segurança 199](#_Toc17904510)

[CA-1: Política e Procedimentos de Avaliação de Segurança e Autorização (P1) 199](#_Toc17904511)

[CA-2: Avaliações de Segurança (P2) 200](#_Toc17904512)

[CA-3: Interconexões do Sistema (P1) 203](#_Toc17904513)

[CA-4: Certificação de Segurança (P0) 205](#_Toc17904514)

[CA-5: Plano de Ação e Marcos (P3) 205](#_Toc17904515)

[CA-6: Autorização de Segurança (P2) 205](#_Toc17904516)

[CA-7: Monitoramento Contínuo (P2) 206](#_Toc17904517)

[CA-8: Treinamento de Invasão (PenTest) (P2) 208](#_Toc17904518)

[CA-9: Conexões do Sistema Interno (P2) 210](#_Toc17904519)

[SC - Proteção de Sistemas e Comunicações 211](#_Toc17904520)

[SC-1: Política e Procedimentos de Proteção de Sistemas e Comunicações (P1) 211](#_Toc17904521)

[SC-2: Particionamento do Aplicativo (P1) 211](#_Toc17904522)

[SC-3: Isolamento das Funções de Segurança (P1) 212](#_Toc17904523)

[SC-4: Informação em Recursos Compartilhados (P1) 214](#_Toc17904524)

[SC-5: Proteção sobre Negação de Serviço (DoS) (P1) 214](#_Toc17904525)

[SC-6: Disponibilidade de Recursos (P0) 216](#_Toc17904526)

[SC-7: Proteção de Borda (P1) 216](#_Toc17904527)

[SC-8: Confidencialidade e Integridade da Transmissão (P1) 222](#_Toc17904528)

[SC-9: Confidencialidade da Transmissão (P0) 224](#_Toc17904529)

[SC-10: Desconexão de Rede (P2) 224](#_Toc17904530)

[SC-11: Caminho Confiável (P0) 224](#_Toc17904531)

[SC-12: Estabelecimento e Gerenciamento de Chaves Criptográficas (P1) 225](#_Toc17904532)

[SC-13: Proteção Criptográfica (P1) 226](#_Toc17904533)

[SC-14: Proteções de Acesso Público (P0) 227](#_Toc17904534)

[SC-15: Dispositivos Colaborativos de Computação (P1) 227](#_Toc17904535)

[SC-16: Transmissão de Atributos de Segurança (P0) 228](#_Toc17904536)

[SC-17: Certificados de Chave Pública da Infraestrutura (P1) 228](#_Toc17904537)

[SC-18: Código Móvel (P2) 228](#_Toc17904538)

[SC-19: Protocolo de Voz por Internet (VOIP) (P1) 230](#_Toc17904539)

[SC-20: Serviço Seguro de Resolução de Nome/Endereço (Fonte Autoritária) (P1) 230](#_Toc17904540)

[SC-21: Serviço Seguro de Resolução de Nome/Endereço (Recursivo ou Caching) (P1) 231](#_Toc17904541)

[SC-22: Arquitetura e Provisão para Serviço de Resolução de Nome/Endereço (P1) 232](#_Toc17904542)

[SC-23: Autenticidade da Sessão (P1) 232](#_Toc17904543)

[SC-24: Falha no Estado Conhecido (P1) 233](#_Toc17904544)

[SC-25: Thin Nodes (P0) 234](#_Toc17904545)

[SC-26: Honeypots (P0) 234](#_Toc17904546)

[SC-27: Aplicações Independentes de Plataforma (P0) 234](#_Toc17904547)

[SC-28: Proteção de Informação em Repouso (P1) 235](#_Toc17904548)

[SC-29: Heterogeneidade (P0) 236](#_Toc17904549)

[SC-30: Ocultamento e Desorientação (P0) 237](#_Toc17904550)

[SC-31: Análise de Canais de Cobertura (P0) 238](#_Toc17904551)

[SC-32: Particionamento do Sistema de Informação (P0) 239](#_Toc17904552)

[SC-33: Integridade da Preparação da Transmissão (P0) 240](#_Toc17904553)

[SC-34: Programas Executáveis não Modificáveis (P0) 240](#_Toc17904554)

[SC-35: Honeyclients (P0) 241](#_Toc17904555)

[SC-36: Processamento e Armazenamento Distribuído (P0) 241](#_Toc17904556)

[SC-37: Canais de Comunicação Fora do Padrão (Out-Of-Band) (P0) 242](#_Toc17904557)

[SC-38: Segurança das Operações (P0) 242](#_Toc17904558)

[SC-39: Isolamento do Processo (P1) 243](#_Toc17904559)

[SC-40: Proteção de Link Sem Fio (P0) 243](#_Toc17904560)

[SC-41: Acesso a Porta e I/O do Dispositivo (P0) 245](#_Toc17904561)

[SC-42: Capacidade do Sensor e Dados (P0) 245](#_Toc17904562)

[SC-43: Restrições de Uso (P0) 246](#_Toc17904563)

[SC-44: Ambiente de Quarentena (P0) 246](#_Toc17904564)

[SI - Integridade de Sistemas e Informação 248](#_Toc17904565)

[SI-1: Política e Procedimentos de Integridade do Sistema e da Informação (P1) 248](#_Toc17904566)

[SI-2: Remediação de Falhas (P1) 248](#_Toc17904567)

[SI-3: Proteção contra Código Malicioso (P1) 250](#_Toc17904568)

[SI-4: Monitoramento do Sistema de Informação (P1) 254](#_Toc17904569)

[SI-5: Alertas, Conselhos e Diretivas de Segurança (P1) 260](#_Toc17904570)

[SI-6: Verificação da Função de Segurança (P1) 261](#_Toc17904571)

[SI-7: Integridade de Software, Firmware e Informação (P1) 261](#_Toc17904572)

[SI-8: Proteção Contra Spam (P2) 265](#_Toc17904573)

[SI-9: Restrições de Entrada de Informação (P0) 266](#_Toc17904574)

[SI-10: Validação de Entrada de Informação (P1) 266](#_Toc17904575)

[SI-11: Controle de Erros (P2) 268](#_Toc17904576)

[SI-12: Manuseio e Controle de Informações (P2) 268](#_Toc17904577)

[SI-13: Prevenção de Falhas Previsíveis (P0) 268](#_Toc17904578)

[SI-14: Não-Persistência (P0) 270](#_Toc17904579)

[SI-15: Filtro de Saída de Informação (P0) 271](#_Toc17904580)

[SI-16: Proteção de Memória (P1) 271](#_Toc17904581)

[SI-17: Procedimentos Seguros (P0) 271](#_Toc17904582)

[SA - Aquisição de Sistemas e Serviços 272](#_Toc17904583)

[SA-1: Política e Procedimentos de Aquisição de Sistemas e Serviços (P1) 272](#_Toc17904584)

[SA-2: Alocação de Recursos (P1) 272](#_Toc17904585)

[SA-3: Ciclo de Vida de Desenvolvimento do Sistema (P1) 273](#_Toc17904586)

[SA-4: Processo de Aquisição (P1) 274](#_Toc17904587)

[SA-5: Documentação do Sistema de Informação (P2) 278](#_Toc17904588)

[SA-6: Restrições de Uso de Software (P0) 280](#_Toc17904589)

[SA-7: Software Instalado pelo Usuário (P0) 280](#_Toc17904590)

[SA-8: Princípios da Engenharia de Segurança (P1) 280](#_Toc17904591)

[SA-9: Serviços Externos do Sistema de Informação (P1) 281](#_Toc17904592)

[SA-10: Gestão da Configuração do Desenvolvedor (P1) 283](#_Toc17904593)

[SA-11: Teste e Avaliação da Segurança do Desenvolvedor (P1) 286](#_Toc17904594)

[SA-12: Proteção da Corrente de Fornecimento (P1) 290](#_Toc17904595)

[SA-13: Confiabilidade (P0) 294](#_Toc17904596)

[SA-14: Análise Crítica (P0) 296](#_Toc17904597)

[SA-15: Processo de Desenvolvimento, Normas e Ferramentas (P2) 296](#_Toc17904598)

[SA-16: Formação Fornecida pelo Desenvolvedor (P2) 300](#_Toc17904599)

[SA-17: Arquitetura e Design de Segurança do Desenvolvedor (P1) 300](#_Toc17904600)

[SA-18: Resistência e Detecção de Manipulação (P0) 303](#_Toc17904601)

[SA-19: Autenticidade do Componente (P0) 304](#_Toc17904602)

[SA-20: Desenvolvimento Personalizado de Componentes Críticos (P0) 305](#_Toc17904603)

[SA-21: Triagem de Desenvolvedores (P0) 305](#_Toc17904604)

[SA-22: Componentes do Sistema Não Suportados (P0) 306](#_Toc17904605)

# AC - Controles de Acesso

## AC-1: Política e Procedimentos de Controle de Acesso (P1)

**Descrição do Controle:**A organização:  
  
a. Desenvolve, documenta e divulga para [Atribuição: pessoal ou funções definidas pela organização]:  
  
1. Uma política de controle de acesso que aborda finalidade, escopo, funções, responsabilidades, comprometimento gerencial, coordenação entre entidades organizacionais e conformidade; e  
  
2. Procedimentos para facilitar a implementação da política de controle de acesso e controles de acesso associados; e  
  
b. Revisa e atualiza a atual:  
  
1. Política de controle de acesso [Atribuição: frequência definida pela organização]; e  
  
2. Procedimentos de controle de acesso [Atribuição: frequência definida pela organização].  
  
**Guia Adicional:**Esse controle aborda o estabelecimento de políticas e procedimentos para a implementação efetiva de controles de segurança selecionados e aprimoramentos de controle na família de CA. As políticas e procedimentos refletem as leis federais aplicáveis, ordens executivas, diretivas, regulamentos, políticas, normas e diretrizes. Políticas e procedimentos do programa de segurança no nível da organização podem tornar desnecessária a necessidade de políticas e procedimentos específicos do sistema. A política pode ser incluída como parte da política geral de segurança da informação para organizações ou, inversamente, pode ser representada por múltiplas políticas refletindo a natureza complexa de certas organizações. Os procedimentos podem ser estabelecidos para o programa de segurança em geral e para sistemas de informação específicos, se necessário. A estratégia de gerenciamento de risco organizacional é um fator chave no estabelecimento de políticas e procedimentos.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-12 | https://csrc.nist.gov/publications/search?keywords-lg=800-12 |
| Publicação Especial NIST 800-100 | https://csrc.nist.gov/publications/search?keywords-lg=800-100 |

## AC-2: Gestão de Conta (P1)

**Descrição do Controle:**A organização:  
  
a. Identifica e seleciona os seguintes tipos de contas do sistema de informações para oferecer suporte a missões / funções de negócios organizacionais: [Atribuição: tipos de contas do sistema de informações definidas pela organização];  
  
b. Atribui gerentes de conta para contas do sistema de informação;  
  
c. Estabelece condições para participação em grupos e funções;  
  
d. Especifica usuários autorizados do sistema de informações, membros de grupos e funções e autorizações de acesso (ou seja, privilégios) e outros atributos (conforme necessário) para cada conta;  
  
e. Requer aprovações por [Atribuição: pessoal ou funções definidas pela organização] para solicitações de criação de contas do sistema de informações;  
  
f. Cria, habilita, modifica, desativa e remove as contas do sistema de informações de acordo com [Atribuição: procedimentos ou condições definidos pela organização];  
  
g. Monitora o uso de contas do sistema de informações;  
  
h. Notifica os gerentes de contas:  
  
1. Quando as contas não são mais necessárias;  
  
2. Quando os usuários são encerrados ou transferidos; e  
  
3. Quando o uso do sistema de informações individuais ou a necessidade de conhecer mudanças;  
  
i. Autoriza o acesso ao sistema de informação baseado em:  
  
1. A autorização de acesso válido;  
  
2. Uso pretendido do sistema; e  
  
3. Outros atributos como exigido pela organização ou associado missões funções / negócios;  
  
j. Comentários responsável por conformidade com os requisitos de gerenciamento de contas [Atribuição: frequência organização definida]; e  
  
k. Estabelece um processo para reemitir de credenciais de conta compartilhada / de grupo (se implantada) quando os indivíduos são removidos do grupo.  
  
**Guia Adicional:**Os tipos de conta do sistema de informações incluem, por exemplo, individual, compartilhado, grupo, sistema, convidado / anônimo, emergência, desenvolvedor / fabricante / fornecedor, temporário e serviço. Alguns dos requisitos de gerenciamento de contas listados acima podem ser implementados pelos sistemas de informações organizacionais. A identificação de usuários autorizados do sistema de informações e a especificação de privilégios de acesso refletem os requisitos em outros controles de segurança no plano de segurança. Os usuários que exigem privilégios administrativos nas contas do sistema de informações recebem uma análise adicional por parte da equipe organizacional apropriada (por exemplo, proprietário do sistema, proprietário da missão / empresa ou diretor de segurança da informação) responsável pela aprovação de tais contas e acesso privilegiado. As organizações podem optar por definir privilégios de acesso ou outros atributos por conta, por tipo de conta ou por uma combinação de ambos. Outros atributos necessários para autorizar o acesso incluem, por exemplo, restrições na hora do dia, no dia da semana e no ponto de origem. Na definição de outros atributos da conta, as organizações consideram os requisitos relacionados ao sistema (por exemplo, manutenção agendada, atualizações do sistema) e os requisitos de missão / negócios (por exemplo, diferenças de fuso horário, requisitos do cliente, acesso remoto para dar suporte aos requisitos de viagem). A não consideração desses fatores pode afetar a disponibilidade do sistema de informações. Contas temporárias e de emergência são contas destinadas a uso a curto prazo. As organizações estabelecem contas temporárias como parte dos procedimentos normais de ativação de contas quando há necessidade de contas de curto prazo sem a demanda por imediatismo na ativação da conta. As organizações estabelecem contas de emergência em resposta a situações de crise e com a necessidade de ativação rápida de conta. Portanto, a ativação de conta de emergência pode ignorar os processos normais de autorização de conta. Contas de emergência e temporárias não devem ser confundidas com contas utilizadas com pouca frequência (por exemplo, contas de login locais usadas para tarefas especiais definidas por organizações ou quando os recursos de rede não estão disponíveis). Essas contas permanecem disponíveis e não estão sujeitas a datas automáticas de desativação ou remoção. As condições para desabilitar ou desativar contas incluem, por exemplo: (i) quando contas compartilhadas / de grupo, de emergência ou temporárias não são mais necessárias; ou (ii) quando indivíduos são transferidos ou demitidos. Alguns tipos de contas do sistema de informações podem exigir treinamento especializado.  
  
**Melhorias do Controle:**

### AC-2(1): Gestão de Conta | Gerenciamento Automatizado da Conta do Sistema

A organização emprega mecanismos automatizados para dar suporte ao gerenciamento de contas do sistema de informações.  
Guia Adicional: O uso de mecanismos automatizados pode incluir, por exemplo: uso de e-mail ou mensagem de texto para notificar automaticamente os gerentes de conta quando os usuários são finalizados ou transferidos; usando o sistema de informações para monitorar o uso da conta; e usando a notificação telefônica para relatar o uso atípico da conta do sistema.

### AC-2(2): Gestão de Conta | Remoção das Contas Temporárias / de Emergência

O sistema de informação automaticamente [Seleção: remove; desativa] contas temporárias e de emergência após [Atribuição: período definido pela organização para cada tipo de conta].  
Guia Adicional: Esse aprimoramento de controle requer a remoção automática de contas temporárias e de emergência automaticamente após um período de tempo predefinido, em vez da conveniência do administrador do sistema.

### AC-2(3): Gestão de Conta | Desativar Contas Inativas

O sistema de informações desabilita automaticamente as contas inativas após [Atribuição: período definido pela organização].

### AC-2(4): Gestão de Conta | Ações de Auditoria Automatizadas

O sistema de informações audita automaticamente as ações de criação, modificação, ativação, desativação e remoção de contas e notifica [Atribuição: pessoal ou funções definidas pela organização].

### AC-2(5): Gestão de Conta | Logout de Inatividade

A organização exige que os usuários efetuem logout quando [Atribuição: período definido pela organização com inatividade prevista ou descrição de quando efetuar logoff].

### AC-2(6): Gestão de Conta | Gestão Dinâmica de Privilégios

O sistema de informações implementa os seguintes recursos de gerenciamento de privilégios dinâmicos: [Atribuição: lista definida pela organização de recursos de gerenciamento de privilégios dinâmicos].  
Guia Adicional: Em contraste com as abordagens convencionais de controle de acesso que empregam contas estáticas do sistema de informações e conjuntos predefinidos de privilégios de usuário, as abordagens dinâmicas de controle de acesso (por exemplo, arquiteturas orientadas a serviços) dependem de decisões de controle de acesso em tempo de execução, facilitadas pelo gerenciamento dinâmico de privilégios. Embora as identidades do usuário possam permanecer relativamente constantes ao longo do tempo, os privilégios do usuário podem mudar com mais frequência com base nos requisitos contínuos da missão / negócios e nas necessidades operacionais das organizações. O gerenciamento dinâmico de privilégios pode incluir, por exemplo, a revogação imediata de privilégios dos usuários, em vez de exigir que os usuários encerrem e reiniciem suas sessões para refletir quaisquer alterações nos privilégios. O gerenciamento dinâmico de privilégios também pode se referir a mecanismos que alteram os privilégios dos usuários com base em regras dinâmicas, em vez de editar perfis de usuário específicos. Esse tipo de gerenciamento de privilégios inclui, por exemplo, ajustes automáticos de privilégios se os usuários estiverem operando fora do horário normal de trabalho ou se os sistemas de informações estiverem sob coação ou em situações de manutenção de emergência. Esse aprimoramento de controle também inclui os efeitos auxiliares das alterações de privilégios, por exemplo, as possíveis alterações nas chaves de criptografia usadas nas comunicações. O gerenciamento dinâmico de privilégios pode suportar requisitos de resiliência do sistema de informações.

### AC-2(7): Gestão de Conta | Regimes Baseados por Cargo

A organização:  
  
a. Estabelece e administra contas de usuário privilegiadas de acordo com um esquema de acesso baseado em funções que organiza o acesso e privilégios permitidos ao sistema de informações em funções;  
  
b. Monitora atribuições de função privilegiadas; e  
  
c. Executa [Atribuição: ações definidas pela organização] quando as atribuições de funções privilegiadas não são mais apropriadas.  
Guia Adicional: Funções privilegiadas são funções definidas pela organização atribuídas a indivíduos que permitem que eles desempenhem determinadas funções relevantes para a segurança que usuários comuns não estão autorizados a desempenhar. Essas funções privilegiadas incluem, por exemplo, gerenciamento de chaves, gerenciamento de contas, administração de rede e sistema, administração de banco de dados e administração da web.

### AC-2(8): Gestão de Conta | Criação de Conta Dinâmica

O sistema de informações cria [Atribuição: contas do sistema de informações definidas pela organização] dinamicamente.  
Guia Adicional: As abordagens dinâmicas para a criação de contas do sistema de informações (por exemplo, conforme implementadas em arquiteturas orientadas a serviços) dependem do estabelecimento de contas (identidades) em tempo de execução para entidades que antes eram desconhecidas. As organizações planejam a criação dinâmica de contas do sistema de informações, estabelecendo mecanismos e relações de confiança com as autoridades apropriadas para validar autorizações e privilégios relacionados.

### AC-2(9): Gestão de Conta | Restrições ao Uso de Contas/Grupos Compartilhados

A organização permite apenas o uso de contas compartilhadas / de grupo que atendem [Atribuição: condições definidas pela organização para estabelecer contas compartilhadas / de grupo].

### AC-2(10): Gestão de Conta | Terminação da Credencial de Contas/Grupos Compartilhados

O sistema de informações encerra as credenciais da conta compartilhada / grupo quando os membros deixam o grupo.

### AC-2(11): Gestão de Conta | Condições de Uso

O sistema de informações aplica [Atribuição: circunstâncias definidas pela organização e/ou condições de uso] para [Atribuição: contas do sistema de informações definidas pela organização].  
Guia Adicional: As organizações podem descrever as condições ou circunstâncias específicas sob as quais as contas do sistema de informações podem ser usadas, por exemplo, restringindo o uso a determinados dias da semana, hora do dia ou durações específicas.

### AC-2(12): Gestão de Conta | Monitoramento de Conta / Uso Atípico

A organização:  
  
a. Monitora as contas do sistema de informações para [Atribuição: uso atípico definido pela organização]; e  
  
b. Informa o uso atípico das contas do sistema de informações para [Atribuição: pessoal ou funções definidas pela organização].  
Guia Adicional: O uso atípico inclui, por exemplo, o acesso a sistemas de informações em determinados horários do dia e em locais que não são consistentes com os padrões normais de uso de pessoas que trabalham em organizações.

### AC-2(13): Gestão de Conta | Desativar Contas para Indivíduos de Alto Risco

A organização desabilita contas de usuários que apresentam um risco significativo dentro de [Atribuição: período definido pela organização] da descoberta do risco.  
Guia Adicional: Os usuários que representam um risco significativo para as organizações incluem indivíduos para os quais evidências ou informações confiáveis indicam a intenção de usar o acesso autorizado aos sistemas de informação para causar danos ou através de quem os adversários causarão danos. O dano inclui potenciais impactos adversos às operações e ativos organizacionais, indivíduos, outras organizações ou a Nação. É essencial uma estreita coordenação entre autoridades autorizadoras, administradores de sistemas de informação e gerentes de recursos humanos, a fim de executar rapidamente esse aprimoramento de controle.

## AC-3: Garantia de Acesso (P1)

**Descrição do Controle:**O sistema de informações impõe autorizações aprovadas para acesso lógico a informações e recursos do sistema de acordo com as políticas de controle de acesso aplicáveis.  
  
**Guia Adicional:**Políticas de controle de acesso (por exemplo, políticas baseadas em identidade, políticas baseadas em funções, matrizes de controle, criptografia) controlam o acesso entre entidades ou assuntos ativos (ou seja, usuários ou processos agindo em nome de usuários) e entidades ou objetos passivos (por exemplo, dispositivos, arquivos, registros, domínios) em sistemas de informação. Além de impor o acesso autorizado no nível do sistema de informações e reconhecer que os sistemas de informação podem hospedar muitos aplicativos e serviços em apoio a missões organizacionais e operações de negócios, os mecanismos de imposição de acesso também podem ser empregados no nível de aplicativo e serviço para fornecer maior segurança das informações.  
  
**Melhorias do Controle:**

### AC-3(1): Garantia de Acesso | Acesso Restrito a Funções Privilegiadas

[Retirado: Incorporado ao AC-6].

### AC-3(2): Garantia de Acesso | Autorização Dupla

O sistema de informações impõe autorização dupla para [Atribuição: comandos privilegiados definidos pela organização e/ou outras ações definidas pela organização].  
Guia Adicional: Mecanismos duplos de autorização exigem a aprovação de dois indivíduos autorizados para execução. As organizações não exigem mecanismos de autorização dupla quando são necessárias respostas imediatas para garantir a segurança pública e ambiental. A autorização dupla também pode ser conhecida como controle de duas pessoas.

### AC-3(3): Garantia de Acesso | Controle Obrigatório de Acesso

O sistema de informações aplica [Atribuição: política de controle de acesso obrigatório definida pela organização] sobre todos os assuntos e objetos em que a política:  
  
a. É aplicada uniformemente em todos os assuntos e objetos dentro dos limites do sistema de informação;  
  
b. Especifica que um assunto ao qual foi concedido acesso às informações é impedido de executar qualquer um dos seguintes procedimentos;  
  
c. Especifica que [Atribuição: assuntos definidos pela organização] pode ser explicitamente concedido [Atribuição: privilégios definidos pela organização (ou seja, são objetos confiáveis)] de forma que não sejam limitados por algumas ou todas as restrições acima.  
Guia Adicional: O controle de acesso obrigatório, conforme definido neste aprimoramento de controle, é sinônimo de controle de acesso não discricionário e não é restrito apenas a certos usos históricos (por exemplo, implementações usando o Modelo Bell-LaPadula). A classe acima de políticas de controle de acesso obrigatório restringe quais ações os indivíduos podem executar com informações obtidas de objetos de dados aos quais eles já receberam acesso, impedindo que eles passem as informações para objetos e objetos não autorizados. Essa classe de políticas obrigatórias de controle de acesso também restringe as ações que os indivíduos podem executar com relação à propagação de privilégios de controle de acesso; isto é, um sujeito com um privilégio não pode passar esse privilégio para outros sujeitos. A política é aplicada uniformemente sobre todos os assuntos e objetos sobre os quais o sistema de informações tem controle. Caso contrário, a política de controle de acesso pode ser contornada. Essa imposição geralmente é fornecida por meio de uma implementação que atende ao conceito de monitor de referência (consulte AC-25). A política é limitada pelo limite do sistema de informações (ou seja, uma vez que as informações são passadas fora do controle do sistema, podem ser necessários meios adicionais para garantir que as restrições nas informações permaneçam em vigor). Os assuntos confiáveis descritos acima recebem privilégios consistentes com o conceito de menor privilégio (consulte AC-6). Os indivíduos de confiança recebem apenas os privilégios mínimos em relação à política acima, necessários para satisfazer as necessidades da missão / negócios da organização. O controle é mais aplicável quando existe algum mandato de política (por exemplo, lei, ordem executiva, diretiva ou regulamento) que estabelece uma política relativa ao acesso a informações sigilosas / classificadas e alguns usuários do sistema de informação não têm acesso autorizado a todas as informações sigilosas / informações classificadas residentes no sistema de informações. Este controle pode operar em conjunto com o AC-3 (4). Um sujeito que é restringido em sua operação por políticas governadas por esse controle ainda pode operar sob as restrições menos rigorosas do AC-3 (4), mas as políticas governadas por esse controle têm precedência sobre as restrições menos rigorosas do AC-3 ( 4) Por exemplo, enquanto uma política de controle de acesso obrigatória impõe uma restrição que impede que um sujeito passe informações para outro sujeito operando com uma etiqueta de sensibilidade diferente, o AC-3 (4) permite que o sujeito passe as informações a qualquer sujeito com a mesma etiqueta de sensibilidade que o sujeito.

### AC-3(4): Garantia de Acesso | Controle de Acesso Discreto

O sistema de informações aplica [Atribuição: política de controle de acesso discricionário definido pela organização] sobre assuntos e objetos definidos, onde a política especifica que um assunto ao qual foi concedido acesso à informação pode executar um ou mais dos seguintes procedimentos:  
  
a. Passe as informações para quaisquer outros assuntos ou objetos;  
  
b. Conceda seus privilégios a outros assuntos;  
  
c. Alterar atributos de segurança em assuntos, objetos, sistema de informações ou componentes do sistema de informações;  
  
d. Escolha os atributos de segurança a serem associados aos objetos recém-criados ou revisados; ou  
  
e. Mude as regras que governam o controle de acesso.  
Guia Adicional: Quando políticas discricionárias de controle de acesso são implementadas, os sujeitos não são limitados com relação a quais ações eles podem executar com informações às quais eles já receberam acesso. Assim, assuntos a quem foi concedido acesso a informações não são impedidos de passar (ou seja, os sujeitos têm o poder de passar) as informações para outros assuntos ou objetos. Este aprimoramento de controle pode operar em conjunto com o AC-3 (3). Um assunto restrito em sua operação pelas políticas regidas pelo AC-3 (3) ainda pode operar sob as restrições menos rigorosas desse aprimoramento de controle. Assim, enquanto o AC-3 (3) impõe restrições que impedem que um sujeito passe informações para outro sujeito operando em um nível de sensibilidade diferente, o AC-3 (4) permite que o sujeito passe as informações para qualquer sujeito no mesmo nível de sensibilidade. A política é limitada pelo limite do sistema de informações. Depois que as informações são passadas fora do controle do sistema de informações, podem ser necessários meios adicionais para garantir que as restrições permaneçam em vigor. Enquanto as definições mais antigas e tradicionais de controle de acesso discricionário requerem controle de acesso baseado em identidade, essa limitação não é necessária para esse uso do controle de acesso discricionário.

### AC-3(5): Garantia de Acesso | Informações Relevantes da Segurança

O sistema de informações impede o acesso a [Atribuição: informações relevantes à segurança definidas pela organização], exceto durante estados seguros e inoperantes do sistema.  
Guia Adicional: Informações relevantes para a segurança são quaisquer informações nos sistemas de informações que possam potencialmente impactar a operação de funções de segurança ou o fornecimento de serviços de segurança de uma maneira que possa resultar em falha no cumprimento das políticas de segurança do sistema ou na manutenção do isolamento de código e dados. As informações relevantes para a segurança incluem, por exemplo, regras de filtragem para roteadores / firewalls, informações sobre gerenciamento de chaves criptográficas, parâmetros de configuração para serviços de segurança e listas de controle de acesso. Os estados do sistema não operacional e seguro incluem os horários em que os sistemas de informação não estão executando o processamento relacionado à missão / negócios (por exemplo, o sistema está offline para manutenção, solução de problemas, inicialização, desligamento).

### AC-3(6): Garantia de Acesso | Proteção das Informações do Usuário e do Sistema

[Retirado: Incorporado ao MP-4 e SC-28].

### AC-3(7): Garantia de Acesso | Controle de Acesso Baseado em Cargo

O sistema de informações impõe uma política de controle de acesso baseada em funções sobre assuntos e objetos definidos e controla o acesso com base em [Atribuição: funções definidas pela organização e usuários autorizados a assumir tais funções].  
Guia Adicional: O controle de acesso baseado em função (RBAC) é uma política de controle de acesso que restringe o acesso do sistema de informações a usuários autorizados. As organizações podem criar funções específicas com base nas funções do trabalho e nas autorizações (ou seja, privilégios) para executar as operações necessárias nos sistemas de informações organizacionais associados às funções definidas pela organização. Quando os usuários são atribuídos às funções organizacionais, eles herdam as autorizações ou privilégios definidos para essas funções. O RBAC simplifica a administração de privilégios para organizações, porque os privilégios não são atribuídos diretamente a todos os usuários (que podem ser um número significativo de indivíduos para organizações de médio a grande porte), mas são adquiridos por meio de atribuições de função. O RBAC pode ser implementado como uma forma obrigatória ou discricionária de controle de acesso. Para organizações que implementam o RBAC com controles de acesso obrigatórios, os requisitos do AC-3 (3) definem o escopo dos assuntos e objetos cobertos pela política.

### AC-3(8): Garantia de Acesso | Revogação das Autorizações de Acesso

O sistema de informações impõe a revogação das autorizações de acesso resultantes de alterações nos atributos de segurança de sujeitos e objetos com base em [Atribuição: regras definidas pela organização que regem o tempo das revogações das autorizações de acesso].  
Guia Adicional: A revogação das regras de acesso pode diferir com base nos tipos de acesso revogados. Por exemplo, se um assunto (ou seja, usuário ou processo) for removido de um grupo, o acesso não poderá ser revogado até a próxima vez que o objeto (por exemplo, arquivo) for aberto ou até a próxima vez que o sujeito tentar um novo acesso ao objeto. A revogação baseada em alterações nas etiquetas de segurança pode entrar em vigor imediatamente. As organizações podem fornecer abordagens alternativas sobre como tornar as revogações imediatas se os sistemas de informação não puderem fornecer essa capacidade e a revogação imediata for necessária.

### AC-3(9): Garantia de Acesso | Lançamento Controlado

O sistema de informações não libera informações fora dos limites estabelecidos, a menos que:  
  
a. A [Atribuição: sistema de informações definido pela organização ou componente do sistema] fornece [Atribuição: salvaguardas de segurança definidas pela organização]; e  
  
b. [Atribuição: salvaguardas de segurança definidas pela organização] são usadas para validar a adequação das informações designadas para liberação.  
Guia Adicional: Os sistemas de informação só podem proteger informações organizacionais dentro dos limites dos limites estabelecidos do sistema. Podem ser necessárias salvaguardas de segurança adicionais para garantir que essas informações sejam adequadamente protegidas depois de ultrapassadas as fronteiras estabelecidas do sistema de informações. Exemplos de informações que saem do limite do sistema incluem a transmissão de informações para um sistema de informações externo ou a impressão das informações em uma de suas impressoras. Nos casos em que o sistema de informação é incapaz de determinar a adequação das proteções fornecidas por entidades fora de seus limites, como controle atenuante, as organizações determinam procedimentalmente se os sistemas de informação externos estão fornecendo segurança adequada. Os meios utilizados para determinar a adequação da segurança fornecida pelos sistemas de informações externos incluem, por exemplo, a realização de inspeções ou testes periódicos, o estabelecimento de acordos entre a organização e suas organizações contrapartes ou algum outro processo. Os meios utilizados por entidades externas para proteger as informações recebidas não precisam ser os mesmos utilizados pela organização, mas os meios empregados são suficientes para fornecer uma adjudicação consistente da política de segurança para proteger as informações. Esse aprimoramento de controle requer que os sistemas de informação empreguem meios técnicos ou procedimentais para validar as informações antes de liberá-las para sistemas externos. Por exemplo, se o sistema de informações transmitir informações para outro sistema controlado por outra organização, serão utilizados meios técnicos para validar que os atributos de segurança associados às informações exportadas sejam apropriados para o sistema receptor. Como alternativa, se o sistema de informações transmitir informações para uma impressora em espaço controlado pela organização, meios procedimentais podem ser empregados para garantir que apenas indivíduos devidamente autorizados tenham acesso à impressora. Esse aprimoramento de controle é mais aplicável quando há algum mandato de política (por exemplo, lei, ordem executiva, diretiva ou regulamento) que estabelece uma política relativa ao acesso às informações, e essa política se aplica além do domínio de um sistema ou organização de informações específico.

### AC-3(10): Garantia de Acesso | Observação Auditada dos Mecanismos de Controle de Acesso

A organização emprega uma substituição auditada dos mecanismos de controle de acesso automatizado em [Atribuição: condições definidas pela organização].

## AC-4: Aplicação do Fluxo de Informação (P1)

**Descrição do Controle:**O sistema de informações impõe autorizações aprovadas para controlar o fluxo de informações dentro do sistema e entre sistemas interconectados baseados em [Atribuição: políticas de controle de fluxo de informações definidas pela organização].  
  
**Guia Adicional:**O controle do fluxo de informações regula onde as informações podem viajar dentro de um sistema de informações e entre sistemas de informações (em oposição a quem tem permissão para acessar as informações) e sem consideração explícita aos acessos subsequentes a essas informações. As restrições de controle de fluxo incluem, por exemplo, impedir que as informações controladas pela exportação sejam transmitidas na Internet para a Internet, bloqueando o tráfego externo que afirma ser de dentro da organização, restringindo solicitações da Web à Internet que não são do servidor proxy da Web interno e limitar as transferências de informações entre organizações com base em estruturas de dados e conteúdo. A transferência de informações entre sistemas de informações que representam diferentes domínios de segurança com diferentes diretivas de segurança apresenta o risco de tais transferências violarem uma ou mais políticas de segurança de domínio. Em tais situações, os proprietários / administradores de informações fornecem orientação em pontos de execução de política designados entre sistemas interconectados. As organizações consideram a exigência de soluções de arquitetura específicas quando necessário para aplicar políticas de segurança específicas. A aplicação inclui, por exemplo: (i) proibir a transferência de informações entre sistemas interconectados (isto é, permitir acesso apenas); (ii) empregar mecanismos de hardware para impor fluxos de informação unidirecionais; e (iii) implementar mecanismos de recondicionamento confiáveis para atribuir novamente atributos de segurança e etiquetas de segurança. As organizações geralmente empregam políticas de controle de fluxo de informações e mecanismos de aplicação para controlar o fluxo de informações entre fontes e destinos designados (por exemplo, redes, indivíduos e dispositivos) nos sistemas de informação e entre sistemas interconectados. O controle de fluxo é baseado nas características da informação e/ou no caminho da informação. A aplicação ocorre, por exemplo, em dispositivos de proteção de limites (por exemplo, gateways, roteadores, proteções, túneis criptografados, firewalls) que empregam conjuntos de regras ou estabelecem configurações que restringem os serviços do sistema de informações, fornecem um recurso de filtragem de pacotes baseado em informações de cabeçalho ou capacidade de filtragem de mensagens com base no conteúdo da mensagem (por exemplo, implementando pesquisas por palavra-chave ou usando características do documento). As organizações também consideram a confiabilidade dos mecanismos de filtragem / inspeção (ou seja, hardware, firmware e componentes de software) que são essenciais para a imposição do fluxo de informações. Os aprimoramentos de controle 3 a 22 atendem principalmente às necessidades de soluções entre domínios, que se concentram em técnicas de filtragem mais avançadas, análise aprofundada e mecanismos mais fortes de aplicação de fluxo implementados em produtos entre domínios, por exemplo, guardas de alta garantia. Tais capacidades geralmente não estão disponíveis em produtos comerciais de tecnologia de prateleira.  
  
**Melhorias do Controle:**

### AC-4(1): Aplicação do Fluxo de Informação | Atributos de Segurança de Objetos

O sistema de informações usa [Atribuição: atributos de segurança definidos pela organização] associado a [Atribuição: objetos de informação, origem e destino definidos pela organização] para aplicar [Atribuição: políticas de controle de fluxo de informações definidas pela organização] como base para decisões de controle de fluxo.  
Guia Adicional: Os mecanismos de aplicação do fluxo de informações comparam os atributos de segurança associados às informações (conteúdo e estrutura dos dados) e aos objetos de origem / destino e respondem adequadamente (por exemplo, bloco, quarentena, administrador de alertas) quando os mecanismos encontram fluxos de informações que não são explicitamente permitidos pelas políticas de fluxo de informações. Por exemplo, um objeto de informação rotulado como Confidencial poderia fluir para um objeto de destino chamado Confidencial, mas um objeto de informação rotulado como Confidencial Crítico não teria permissão para fluir para um objeto de destino rotulado como Confidencial. Os atributos de segurança também podem incluir, por exemplo, endereços de origem e destino empregados em firewalls de filtro de tráfego. A imposição de fluxo usando atributos explícitos de segurança pode ser usada, por exemplo, para controlar a liberação de certos tipos de informações.

### AC-4(2): Aplicação do Fluxo de Informação | Domínios de Processamento

O sistema de informações usa domínios de processamento protegidos para impor [Atribuição: políticas de controle de fluxo de informações definidas pela organização] como base para decisões de controle de fluxo.  
Guia Adicional: Nos sistemas de informações, os domínios de processamento protegidos são espaços de processamento que possuem interações controladas com outros espaços de processamento, permitindo o controle dos fluxos de informações entre esses espaços e para / de objetos de dados / informações. Um domínio de processamento protegido pode ser fornecido, por exemplo, implementando a imposição de domínio e tipo. Na imposição de domínio e tipo, os processos do sistema de informações são atribuídos aos domínios; as informações são identificadas por tipos; e os fluxos de informações são controlados com base nos acessos a informações permitidos (determinados por domínio e tipo), sinalização permitida entre domínios e transições de processo permitidas para outros domínios.

### AC-4(3): Aplicação do Fluxo de Informação | Controle de Fluxo de Informação Dinâmica

O sistema de informações aplica controle dinâmico do fluxo de informações com base em [Atribuição: políticas definidas pela organização].  
Guia Adicional: As políticas organizacionais relacionadas ao controle dinâmico do fluxo de informações incluem, por exemplo, permitir ou não fluxos de informações com base em condições variáveis ou considerações de missão / operação. As condições de mudança incluem, por exemplo, mudanças na tolerância ao risco organizacional devido a mudanças no imediatismo das necessidades da missão / negócios, mudanças no ambiente de ameaças e detecção de eventos potencialmente prejudiciais ou adversos.

### AC-4(4): Aplicação do Fluxo de Informação | Verificação de Conteúdo das Informações Criptografadas

O sistema de informações evita que as informações criptografadas ignorem os mecanismos de verificação de conteúdo [Seleção (uma ou mais): descriptografando as informações; bloquear o fluxo da informação criptografada; encerrar sessões de comunicação tentando transmitir informações criptografadas; [Atribuição: procedimento ou método definido pela organização]].

### AC-4(5): Aplicação do Fluxo de Informação | Tipos de Dados Incorporados

O sistema de informações aplica [Atribuição: limitações definidas pela organização] na incorporação de tipos de dados em outros tipos de dados.  
Guia Adicional: A incorporação de tipos de dados em outros tipos de dados pode resultar em eficácia reduzida do controle de fluxo. A incorporação de tipo de dados inclui, por exemplo, inserção de arquivos executáveis como objetos em arquivos de processamento de texto, inserção de referências ou informações descritivas em um arquivo de mídia e tipos de dados compactados ou arquivados que podem incluir vários tipos de dados incorporados. As limitações na incorporação de tipos de dados consideram os níveis de incorporação e proíbem os níveis de incorporação de tipos de dados que estão além da capacidade das ferramentas de inspeção.

### AC-4(6): Aplicação do Fluxo de Informação | Metadata

O sistema de informações aplica o controle do fluxo de informações com base em [Atribuição: metadados definidos pela organização].  
Guia Adicional: Metadados são informações usadas para descrever as características dos dados. Os metadados podem incluir metadados estruturais que descrevem estruturas de dados (por exemplo, formato de dados, sintaxe e semântica) ou metadados descritivos que descrevem o conteúdo dos dados (por exemplo, idade, localização, número de telefone). A imposição de fluxos de informações permitidos com base em metadados permite um controle de fluxo mais simples e eficaz. As organizações consideram a confiabilidade dos metadados no que diz respeito à precisão dos dados (ou seja, conhecimento de que os valores dos metadados estão corretos em relação aos dados), integridade dos dados (ou seja, proteção contra alterações não autorizadas nas tags de metadados) e a ligação dos metadados aos dados carga útil (ou seja, garantir técnicas de encadernação suficientemente fortes com níveis adequados de garantia).

### AC-4(7): Aplicação do Fluxo de Informação | Mecanismos de Fluxo Unidirecionais

O sistema de informações aplica [Atribuição: fluxos de informações unidirecionais definidos pela organização] usando mecanismos de hardware.

### AC-4(8): Aplicação do Fluxo de Informação | Filtros de Política de Segurança

O sistema de informações aplica o controle do fluxo de informações usando [Atribuição: filtros de política de segurança definidos pela organização] como base para decisões de controle de fluxo para [Atribuição: fluxos de informações definidos pela organização].  
Guia Adicional: Os filtros de política de segurança definidos pela organização podem abordar estruturas e conteúdo de dados. Por exemplo, os filtros de política de segurança para estruturas de dados podem verificar comprimentos máximos de arquivo, tamanhos máximos de campo e tipos de dados / arquivo (para dados estruturados e não estruturados). Os filtros da política de segurança para conteúdo de dados podem verificar palavras específicas (por exemplo, filtros de palavras sujas / limpas), valores enumerados ou intervalos de valores de dados e conteúdo oculto. Os dados estruturados permitem a interpretação do conteúdo dos dados pelos aplicativos. Dados não estruturados geralmente se referem a informações digitais sem uma estrutura de dados específica ou com uma estrutura de dados que não facilita o desenvolvimento de conjuntos de regras para abordar a sensibilidade específica das informações transmitidas pelos dados ou pelas decisões de execução de fluxo associadas. Os dados não estruturados consistem em: (i) objetos de bitmap que são inerentemente não baseados em idioma (por exemplo, arquivos de imagem, vídeo ou áudio); e (ii) objetos de texto baseados em idiomas escritos ou impressos (por exemplo, documentos comerciais prontos para processamento de texto, planilhas ou e-mails). As organizações podem implementar mais de um filtro de política de segurança para atender aos objetivos de controle do fluxo de informações (por exemplo, empregar listas de palavras limpas em conjunto com listas de palavras sujas pode ajudar a reduzir falsos positivos).

### AC-4(9): Aplicação do Fluxo de Informação | Revisões Humanas

O sistema de informações impõe o uso de revisões humanas para [Atribuição: fluxos de informações definidos pela organização] sob as seguintes condições: [Atribuição: condições definidas pela organização].  
Guia Adicional: As organizações definem filtros de política de segurança para todas as situações em que são possíveis decisões automatizadas de controle de fluxo. Quando uma decisão de controle de fluxo totalmente automatizada não é possível, uma revisão humana pode ser empregada em substituição ou como um complemento à filtragem automatizada de políticas de segurança. As análises humanas também podem ser empregadas conforme necessário pelas organizações.

### AC-4(10): Aplicação do Fluxo de Informação | Ativar/Desativar Filtros de Política de Segurança

O sistema de informações fornece aos administradores privilegiados a capacidade de ativar / desativar [Atribuição: filtros de política de segurança definidos pela organização] sob as seguintes condições: [Atribuição: condições definidas pela organização].  
Guia Adicional: Por exemplo, conforme permitido pela autorização do sistema de informações, os administradores podem ativar os filtros de política de segurança para acomodar os tipos de dados aprovados.

### AC-4(11): Aplicação do Fluxo de Informação | Configuração de Filtros de Política de Segurança

O sistema de informações oferece aos administradores privilegiados a capacidade de [Atribuição: filtros de política de segurança definidos pela organização] para oferecer suporte a diferentes políticas de segurança.  
Guia Adicional: Por exemplo, para refletir alterações nas políticas de segurança, os administradores podem alterar a lista de "palavras sujas" que os mecanismos da política de segurança verificam de acordo com as definições fornecidas pelas organizações.

### AC-4(12): Aplicação do Fluxo de Informação | Identificadores do Tipo de Dados

O sistema de informações, ao transferir informações entre diferentes domínios de segurança, usa [Atribuição: identificadores de tipo de dados definidos pela organização] para validar dados essenciais para decisões de fluxo de informações.  
Guia Adicional: Os identificadores de tipo de dados incluem, por exemplo, nomes de arquivos, tipos de arquivos, assinaturas / tokens de arquivos e várias assinaturas / tokens de arquivos internos. Os sistemas de informação podem permitir a transferência de dados somente se estiverem em conformidade com as especificações de formato de tipo de dados.

### AC-4(13): Aplicação do Fluxo de Informação | Decomposição em Subcomponentes Relevantes da Política

O sistema de informações, ao transferir informações entre diferentes domínios de segurança, decompõe as informações em [Atribuição: subcomponentes relevantes à política definida pela organização] para submissão aos mecanismos de imposição de políticas.  
Guia Adicional: Os mecanismos de imposição de políticas aplicam regras de filtragem, inspeção e/ou sanitização aos subcomponentes de informações relevantes para a política, a fim de facilitar a imposição do fluxo antes de transferir essas informações para diferentes domínios de segurança. A análise de arquivos de transferência facilita as decisões de política sobre origem, destino, certificados, classificação, anexos e outros diferenciadores de componentes relacionados à segurança.

### AC-4(14): Aplicação do Fluxo de Informação | Restrições dos Filtro da Política de Segurança

O sistema de informações, ao transferir informações entre diferentes domínios de segurança, implementa [Atribuição: filtros de política de segurança definidos pela organização], exigindo formatos totalmente enumerados que restringem a estrutura e o conteúdo dos dados.  
Guia Adicional: A estrutura de dados e as restrições de conteúdo reduzem o leque de possíveis conteúdos maliciosos e/ou não autorizados em transações entre domínios. Os filtros de política de segurança que restringem as estruturas de dados incluem, por exemplo, a restrição de tamanhos de arquivo e tamanhos de campo. Os filtros da política de conteúdo de dados incluem, por exemplo: (i) formatos de codificação para conjuntos de caracteres (por exemplo, Formatos de transformação de conjuntos de caracteres universais, Código Padrão Americano para Intercâmbio de Informações); (ii) restringir os campos de dados de caracteres para conter apenas caracteres alfanuméricos; (iii) proibir caracteres especiais; e (iv) validar estruturas de esquema.

### AC-4(15): Aplicação do Fluxo de Informação | Detecção de Informações Não Inseridas

O sistema de informações, ao transferir informações entre diferentes domínios de segurança, examina as informações quanto à presença de [Atribuição: informações não autorizadas definidas pela organização] e proíbe a transferência dessas informações de acordo com a [Atribuição: política de segurança definida pela organização].  
Guia Adicional: A detecção de informações não autorizadas inclui, por exemplo, a verificação de todas as informações a serem transferidas para códigos maliciosos e palavras sujas.

### AC-4(16): Aplicação do Fluxo de Informação | Transferências de Informação em Sistemas Interligados

[Retirado: Incorporado ao AC-4].

### AC-4(17): Aplicação do Fluxo de Informação | Autenticação de Domínio

O sistema de informações identifica e autentica exclusivamente os pontos de origem e destino por [Seleção (um ou mais): organização, sistema, aplicativo, indivíduo] para transferência de informações.  
Guia Adicional: A atribuição é um componente crítico de um conceito de segurança de operações. A capacidade de identificar pontos de origem e destino das informações que fluem nos sistemas de informações, permite a reconstrução forense de eventos quando necessário e incentiva a conformidade com as políticas atribuindo violações das políticas a organizações / indivíduos específicos. A autenticação de domínio bem-sucedida exige que os rótulos do sistema de informações façam a distinção entre sistemas, organizações e indivíduos envolvidos na preparação, envio, recebimento ou disseminação de informações.

### AC-4(18): Aplicação do Fluxo de Informação | Ligação dos Atributos da Segurança

O sistema de informações vincula os atributos de segurança às informações usando [Atribuição: técnicas de ligação definidas pela organização] para facilitar a aplicação da política de fluxo de informações.  
Guia Adicional: As técnicas de ligação implementadas pelos sistemas de informações afetam a força da ligação dos atributos de segurança às informações. A força de ligação e a garantia associada às técnicas de ligação desempenham um papel importante na confiança das organizações no processo de aplicação do fluxo de informações. As técnicas de encadernação afetam o número e o grau de revisões adicionais exigidas pelas organizações.

### AC-4(19): Aplicação do Fluxo de Informação | Validação de Metadata

O sistema de informações, ao transferir informações entre diferentes domínios de segurança, aplica a mesma filtragem de política de segurança aos metadados que se aplica às cargas úteis de dados.  
Guia Adicional: Esse aprimoramento de controle requer a validação de metadados e os dados aos quais os metadados se aplicam. Algumas organizações distinguem entre metadados e cargas úteis de dados (ou seja, apenas os dados aos quais os metadados estão vinculados). Outras organizações não fazem essas distinções, considerando os metadados e os dados aos quais os metadados se aplicam como parte da carga útil. Todas as informações (incluindo os metadados e os dados aos quais os metadados se aplicam) estão sujeitas a filtragem e inspeção.

### AC-4(20): Aplicação do Fluxo de Informação | Soluções Aprovadas

A organização emprega [Atribuição: soluções definidas pela organização em configurações aprovadas] para controlar o fluxo de [Atribuição: informações definidas pela organização] entre domínios de segurança.  
Guia Adicional: As organizações definem soluções e configurações aprovadas em políticas e diretrizes entre domínios, de acordo com os tipos de fluxos de informações através dos limites da classificação. O Escritório de Gerenciamento Unificado entre Domínios (UCDMO) fornece uma lista de base das soluções aprovadas entre domínios.

### AC-4(21): Aplicação do Fluxo de Informação | Separação Física / Lógica dos Fluxos de Informação

O sistema de informações separa os fluxos de informações lógica ou fisicamente usando [Atribuição: mecanismos e/ou técnicas definidas pela organização] para realizar [Atribuição: separações necessárias definidas pela organização por tipos de informação].  
Guia Adicional: A imposição da separação de fluxos de informações por tipo pode aumentar a proteção, garantindo que as informações não sejam misturadas enquanto em trânsito e permitindo o controle de fluxo por caminhos de transmissão que talvez não sejam alcançáveis. Os tipos de informações separáveis incluem, por exemplo, tráfego de comunicações de entrada e saída, solicitações e respostas de serviço e informações de diferentes categorias de segurança.

### AC-4(22): Aplicação do Fluxo de Informação | Somente Acesso

O sistema de informações fornece acesso a partir de um único dispositivo a plataformas, aplicativos ou dados de computação residentes em vários domínios de segurança diferentes, impedindo qualquer fluxo de informações entre os diferentes domínios de segurança.  
Guia Adicional: O sistema de informações, por exemplo, fornece uma área de trabalho para os usuários acessarem cada domínio de segurança conectado sem fornecer mecanismos para permitir a transferência de informações entre os diferentes domínios de segurança.

## AC-5: Segregação de Funções (P1)

**Descrição do Controle:**A organização:  
  
a. Separa [Tarefa: deveres definidos pela organização dos indivíduos];  
  
b. Documentos separação de deveres de indivíduos; e  
  
c. Define autorizações de acesso ao sistema de informações para suportar a separação de tarefas.  
  
**Guia Adicional:**A separação de tarefas aborda o potencial de abuso de privilégios autorizados e ajuda a reduzir o risco de atividade maléfica sem conluio. A separação de tarefas inclui, por exemplo: (i) divisão de funções da missão e funções de suporte do sistema de informações entre diferentes indivíduos e/ou funções; (ii) condução de funções de suporte de sistemas de informação com diferentes indivíduos (por exemplo, gerenciamento de sistemas, programação, gerenciamento de configurações, garantia e teste de qualidade e segurança de rede); e (iii) garantir que o pessoal de segurança que administra as funções de controle de acesso também não administre as funções de auditoria.

## AC-6: Menor Privilégio (P1)

**Descrição do Controle:**A organização emprega o princípio de privilégio mínimo, permitindo somente acessos autorizados para usuários (ou processos agindo em nome de usuários) que são necessários para realizar tarefas atribuídas de acordo com as missões organizacionais e funções de negócios.  
  
**Guia Adicional:**As organizações empregam menos privilégios para tarefas e sistemas de informação específicos. O princípio do menor privilégio também é aplicado aos processos do sistema de informações, garantindo que os processos operem em níveis de privilégios não superiores aos necessários para realizar as missões organizacionais / funções de negócios necessárias. As organizações consideram a criação de processos, funções e contas do sistema de informações adicionais, conforme necessário, para obter o mínimo privilégio. As organizações também aplicam o menor privilégio ao desenvolvimento, implementação e operação de sistemas de informações organizacionais.  
  
**Melhorias do Controle:**

### AC-6(1): Menor Privilégio | Autorizar o Acesso à Funções de Segurança

A organização autoriza explicitamente o acesso a [Atribuição: funções de segurança definidas pela organização (implantadas em hardware, software e firmware) e informações relevantes à segurança].  
Guia Adicional: As funções de segurança incluem, por exemplo, estabelecimento de contas do sistema, configuração de autorizações de acesso (ou seja, permissões, privilégios), configuração de eventos a serem auditados e configuração de parâmetros de detecção de intrusão. As informações relevantes para a segurança incluem, por exemplo, regras de filtragem para roteadores / firewalls, informações sobre gerenciamento de chaves criptográficas, parâmetros de configuração para serviços de segurança e listas de controle de acesso. O pessoal explicitamente autorizado inclui, por exemplo, administradores de segurança, administradores de sistemas e redes, agentes de segurança do sistema, pessoal de manutenção do sistema, programadores de sistema e outros usuários privilegiados.

### AC-6(2): Menor Privilégio | Acesso Não Privilegiado a Funções Não Segurança

A organização exige que os usuários de contas ou funções do sistema de informações com acesso a [Atribuição: funções de segurança definidas pela organização ou informações relevantes à segurança] usem contas ou funções não privilegiadas ao acessar funções não seguras.  
Guia Adicional: Esse aprimoramento de controle limita a exposição ao operar em contas ou funções privilegiadas. A inclusão de funções aborda situações em que as organizações implementam políticas de controle de acesso, como controle de acesso baseado em função e onde uma mudança de função fornece o mesmo grau de garantia na alteração das autorizações de acesso para o usuário e todos os processos que agem em nome do usuário como seria proporcionado por uma alteração entre uma conta privilegiada e não privilegiada.

### AC-6(3): Menor Privilégio | Acesso aos Comandos Privilegiados de Rede

A organização autoriza o acesso da rede a [Atribuição: comandos privilegiados definidos pela organização] apenas para [Atribuição: necessidades operacionais obrigatórias definidas pela organização] e documenta a justificativa para esse acesso no plano de segurança do sistema de informações.  
Guia Adicional: Acesso à rede é qualquer acesso através de uma conexão de rede em vez do acesso local (ou seja, o usuário estar fisicamente presente no dispositivo).

### AC-6(4): Menor Privilégio | Domínios Separados de Processamento

O sistema de informações fornece domínios de processamento separados para permitir uma alocação mais refinada de privilégios de usuário.  
Guia Adicional: O fornecimento de domínios de processamento separados para alocação mais refinada de privilégios de usuário inclui, por exemplo: (i) o uso de técnicas de virtualização para permitir privilégios adicionais em uma máquina virtual enquanto restringe privilégios a outras máquinas virtuais ou à máquina real subjacente; (ii) empregar mecanismos de separação de domínio de hardware e/ou software; e (iii) implementar domínios físicos separados.

### AC-6(5): Menor Privilégio | Contas Privilegiadas

A organização restringe contas privilegiadas no sistema de informações a [Atribuição: pessoal ou funções definidas pela organização].  
Guia Adicional: Contas privilegiadas, incluindo contas de super usuário, são normalmente descritas como administrador do sistema para vários tipos de sistemas operacionais comerciais prontos para uso. A restrição de contas privilegiadas a pessoas ou funções específicas impede que os usuários diários tenham acesso a informações / funções privilegiadas. As organizações podem diferenciar na aplicação desse aprimoramento de controle entre privilégios permitidos para contas locais e contas de domínio, desde que as organizações mantenham a capacidade de controlar as configurações do sistema de informações para os principais parâmetros de segurança e, se necessário, para mitigar suficientemente os riscos.

### AC-6(6): Menor Privilégio | Acesso Privilegiado por Usuários Não Organizacionais

A organização proíbe o acesso privilegiado ao sistema de informações por usuários não organizacionais.

### AC-6(7): Menor Privilégio | Revisão dos Privilégios do Usuário

A organização:  
  
a. Revisa [Atribuição: frequência definida pela organização] os privilégios atribuídos a [Atribuição: funções ou classes de usuários definidas pela organização] para validar a necessidade de tais privilégios; e  
  
b. Atribui novamente ou remove privilégios, se necessário, para refletir corretamente a missão organizacional / necessidades de negócios.  
Guia Adicional: A necessidade de certos privilégios de usuário atribuídos pode mudar com o tempo, refletindo alterações nas missões organizacionais / função comercial, ambientes de operação, tecnologias ou ameaças. A revisão periódica dos privilégios de usuário atribuídos é necessária para determinar se a justificativa para atribuir esses privilégios permanece válida. Se a necessidade não puder ser revalidada, as organizações tomarão as ações corretivas apropriadas.

### AC-6(8): Menor Privilégio | Níveis de Privilégio para Execução de Código

O sistema de informações impede que [Atribuição: software definido pela organização] seja executado em níveis de privilégios mais altos do que os usuários que executam o software.  
Guia Adicional: Em certas situações, os aplicativos / programas de software precisam ser executados com privilégios elevados para executar as funções necessárias. No entanto, se os privilégios necessários para a execução estiverem em um nível superior aos privilégios atribuídos aos usuários organizacionais que invocam esses aplicativos / programas, esses usuários receberão indiretamente mais privilégios do que os atribuídos pelas organizações.

### AC-6(9): Menor Privilégio | Auditoria do Uso de Funções Privilegiadas

O sistema de informação audita a execução de funções privilegiadas.  
Guia Adicional: O uso indevido de funções privilegiadas, intencionalmente ou não, por usuários autorizados ou por entidades externas não autorizadas que tenham comprometido as contas do sistema de informações, é uma preocupação séria e contínua e pode ter impactos adversos significativos nas organizações. A auditoria do uso de funções privilegiadas é uma maneira de detectar esse uso indevido e, ao fazer isso, ajuda a reduzir o risco de ameaças internas e a ameaça persistente avançada (APT).

### AC-6(10): Menor Privilégio | Proibir Usuários Não Privilegiados de Executar Funções Privilegiadas

O sistema de informações impede que usuários não privilegiados executem funções privilegiadas para incluir a desativação, contornar ou alterar as salvaguardas / contramedidas de segurança implementadas.  
Guia Adicional: As funções privilegiadas incluem, por exemplo, o estabelecimento de contas do sistema de informações, a execução de verificações de integridade do sistema ou a administração de atividades de gerenciamento de chaves criptográficas. Usuários não privilegiados são indivíduos que não possuem autorizações apropriadas. Contornar os mecanismos de detecção e prevenção de intrusões ou mecanismos maliciosos de proteção de código são exemplos de funções privilegiadas que exigem proteção de usuários não privilegiados.

## AC-7: Tentativas de Login Incorretas (P2)

**Descrição do Controle:**O sistema de informação:  
  
a. Impõe um limite de [Atribuição: número definido pela organização] tentativas de login inválido consecutivas por um usuário durante uma [Atribuição: período de tempo definido pela organização]; e  
  
b. Automaticamente [Seleção: bloqueia a conta / nó para uma [Atribuição: período de tempo definido pela organização]; bloqueia a conta / nó até ser liberado por um administrador; Atrasos próximo prompt de login de acordo com [Atribuição: algoritmo de atraso definido pela organização]] quando o número máximo de tentativas malsucedidas é excedido.  
  
**Guia Adicional:**Esse controle se aplica independentemente de o login ocorrer por meio de uma conexão local ou de rede. Devido ao potencial de negação de serviço, os bloqueios automáticos iniciados pelos sistemas de informações são geralmente temporários e liberados automaticamente após um período de tempo predeterminado estabelecido pelas organizações. Se um algoritmo de atraso for selecionado, as organizações poderão optar por empregar algoritmos diferentes para diferentes componentes do sistema de informação com base nos recursos desses componentes. As respostas às tentativas malsucedidas de login podem ser implementadas nos níveis de sistema operacional e aplicativo.  
  
**Melhorias do Controle:**

### AC-7(1): Tentativas de Login Incorretas | Bloqueio de Conta Automático

[Retirado: Incorporado ao AC-7].

### AC-7(2): Tentativas de Login Incorretas | Limpeza/Wipe de Dispositivo Móvel

O sistema de informações limpa / limpa as informações de [Atribuição: dispositivos móveis definidos pela organização] com base em [Atribuição: requisitos / técnicas de limpeza / limpeza definidas pela organização] após [Atribuição: número definido pela organização] tentativas consecutivas sem êxito de login do dispositivo.  
Guia Adicional: Esse aprimoramento de controle se aplica apenas a dispositivos móveis para os quais ocorre um login (por exemplo, assistentes digitais pessoais, smartphones, tablets). O login é para o dispositivo móvel, não para nenhuma conta no dispositivo. Portanto, logins bem-sucedidos em qualquer conta em dispositivos móveis redefinem a contagem malsucedida de login para zero. As organizações definem as informações a serem limpas / limpas com cuidado, a fim de evitar purgas / limpezas excessivas, o que pode resultar na inutilização dos dispositivos. A limpeza / limpeza pode ser desnecessária se as informações no dispositivo estiverem protegidas com mecanismos de criptografia suficientemente fortes.

## AC-8: Notificação de Utilização do Sistema (P1)

**Descrição do Controle:**O sistema de informação:  
  
a. Exibe para os usuários [Atribuição: mensagem ou banner de notificação de uso do sistema definido pela organização] antes de conceder acesso ao sistema que fornece avisos de privacidade e segurança consistentes com as leis federais, ordens executivas, diretivas, políticas, regulamentos, normas e diretrizes aplicáveis e declara que :  
  
1. Os usuários estão acessando um sistema de informações do governo dos EUA;  
  
2. O uso do sistema de informação pode ser monitorado, registrado e sujeito a auditoria;  
  
3. O uso não autorizado do sistema de informação é proibido e sujeito a penalidades criminais e civis; e  
  
4. O uso do sistema de informação indica consentimento para monitoramento e registro;  
  
b. Mantém a mensagem ou banner de notificação na tela até que os usuários reconheçam as condições de uso e executem ações explícitas para efetuar login ou acessar mais o sistema de informações; e  
  
c. Para sistemas publicamente acessíveis:  
  
1. Exibe informações de uso do sistema [Atribuição: condições definidas pela organização], antes de conceder acesso adicional;  
  
2. Exibe referências, se houver, ao monitoramento, gravação ou auditoria que são consistentes com as acomodações de privacidade de tais sistemas que geralmente proíbem essas atividades; e  
  
3. Inclui uma descrição dos usos autorizados do sistema.  
  
**Guia Adicional:**As notificações de uso do sistema podem ser implementadas usando mensagens ou banners de aviso exibidos antes que as pessoas efetuem login nos sistemas de informação. As notificações de uso do sistema são usadas somente para acesso via interfaces de login com usuários humanos e não são necessárias quando tais interfaces humanas não existem. As organizações consideram mensagens / banners de notificação de uso do sistema exibidos em vários idiomas com base nas necessidades organizacionais específicas e na demografia dos usuários do sistema de informações. As organizações também consultam o Escritório do Conselho Geral para revisão legal e aprovação do conteúdo do banner de aviso.

## AC-9: Notificação de Login Anterior (Acesso) (P0)

**Descrição do Controle:**O sistema de informações notifica o usuário, após o login bem-sucedido (acesso) ao sistema, da data e hora do último login (acesso).  
  
**Guia Adicional:**Esse controle é aplicável a logins para sistemas de informações por meio de interfaces com o usuário e logins humanos para sistemas que ocorrem em outros tipos de arquiteturas (por exemplo, arquiteturas orientadas a serviços).  
  
**Melhorias do Controle:**

### AC-9(1): Notificação de Login Anterior (Acesso) | Logs Inúteis

O sistema de informações notifica o usuário, após o login / acesso bem-sucedido, do número de tentativas malsucedidas de login / acesso desde o último login / acesso bem-sucedido.

### AC-9(2): Notificação de Login Anterior (Acesso) | Logins Bem-Sucedidos / Não Sucedidos

O sistema de informação notifica o usuário do número de [Seleção: logins / acessos bem-sucedidos; tentativas malsucedidas de login / acesso; ambos] durante [Atribuição: período definido pela organização].

### AC-9(3): Notificação de Login Anterior (Acesso) | Notificação sobre Alterações de Conta

O sistema de informações notifica o usuário sobre alterações em [Atribuição: características / parâmetros relacionados à segurança definidos pela organização da conta do usuário] durante [Atribuição: período definido pela organização].

### AC-9(4): Notificação de Login Anterior (Acesso) | Informações Adicionais de Login

O sistema de informações notifica o usuário, após o login (acesso) bem-sucedido, das seguintes informações adicionais: [Atribuição: informações definidas pela organização a serem incluídas além da data e hora do último login (acesso)].  
Guia Adicional: Esse aprimoramento de controle permite que as organizações especifiquem informações adicionais a serem fornecidas aos usuários no login, incluindo, por exemplo, o local do último login. A localização do usuário é definida como a informação que pode ser determinada pelos sistemas de informação, por exemplo, endereços IP dos quais ocorreram logins na rede, identificadores de dispositivo ou notificações de logins locais.

## AC-10: Controle de Sessões Simultâneas (P3)

**Descrição do Controle:**O sistema de informações limita o número de sessões simultâneas para cada [Atribuição: conta definida pela organização e/ou tipo de conta] para [Atribuição: número definido pela organização].  
  
**Guia Adicional:**As organizações podem definir o número máximo de sessões simultâneas para as contas do sistema de informações globalmente, por tipo de conta (por exemplo, usuário privilegiado, usuário não privilegiado, domínio, aplicativo específico), por conta ou uma combinação. Por exemplo, as organizações podem limitar o número de sessões simultâneas para administradores de sistema ou indivíduos que trabalham em domínios particularmente sensíveis ou aplicativos de missão crítica. Esse controle aborda sessões simultâneas para contas do sistema de informações e não aborda sessões simultâneas de usuários únicos por meio de várias contas do sistema.

## AC-11: Bloqueio da Sessão (P3)

**Descrição do Controle:**O sistema de informação:  
  
a. Impede ainda mais acesso ao sistema, iniciando um bloqueio de sessão após [Atribuição: período de tempo definido pela organização] de inatividade ou ao receber uma solicitação de um usuário; e  
  
b. Mantém o bloqueio da sessão até o usuário restabelecer o acesso usando os procedimentos de identificação e autenticação estabelecidos.  
  
**Guia Adicional:**Os bloqueios de sessão são ações temporárias executadas quando os usuários param de trabalhar e se afastam da vizinhança imediata dos sistemas de informações, mas não desejam efetuar logout devido à natureza temporária de suas ausências. Os bloqueios de sessão são implementados onde as atividades da sessão podem ser determinadas. Isso geralmente é no nível do sistema operacional, mas também pode estar no nível do aplicativo. Os bloqueios de sessão não são um substituto aceitável para efetuar logoff dos sistemas de informações, por exemplo, se as organizações exigirem que os usuários efetuem logoff no final dos dias úteis.  
  
**Melhorias do Controle:**

### AC-11(1): Bloqueio da Sessão | Proteção de Tela

O sistema de informações oculta, através do bloqueio da sessão, informações previamente visíveis no visor com uma imagem visível publicamente.  
Guia Adicional: As imagens publicamente visíveis podem incluir imagens estáticas ou dinâmicas, por exemplo, padrões usados com protetores de tela, imagens fotográficas, cores sólidas, relógio, indicador de duração da bateria ou uma tela em branco, com a ressalva adicional de que nenhuma das imagens transmite informações confidenciais.

**Referências:**

|  |  |
| --- | --- |
| OMB Memorando 06-16 | https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2006/m06-16.pdf |

## AC-12: Encerramento da Sessão (P2)

**Descrição do Controle:**O sistema de informações encerra automaticamente uma sessão do usuário após [Atribuição: condições definidas pela organização ou eventos de acionador que exigem desconexão da sessão].  
  
**Guia Adicional:**Esse controle aborda a finalização de sessões lógicas iniciadas pelo usuário, em contraste com o SC-10, que aborda a finalização de conexões de rede associadas a sessões de comunicação (ou seja, desconexão da rede). Uma sessão lógica (para acesso local, de rede e remoto) é iniciada sempre que um usuário (ou processo agindo em nome de um usuário) acessa um sistema de informações organizacionais. Essas sessões do usuário podem ser encerradas (e, portanto, encerrar o acesso do usuário) sem encerrar as sessões da rede. A finalização da sessão finaliza todos os processos associados à sessão lógica de um usuário, exceto aqueles criados especificamente pelo usuário (ou seja, proprietário da sessão) para continuar após o término da sessão. As condições ou eventos de acionamento que exigem o encerramento automático da sessão podem incluir, por exemplo, períodos de inatividade do usuário definidos pela organização, respostas direcionadas a certos tipos de incidentes, restrições de horário do uso do sistema de informações.  
  
**Melhorias do Controle:**

### AC-12(1): Encerramento da Sessão | Mensagem Exibida quando Usuário Efetua Logout

O sistema de informação:  
  
a. Fornece um recurso de logout para sessões de comunicação iniciadas pelo usuário sempre que a autenticação é usada para obter acesso a [Atribuição: recursos de informação definidos pela organização]; e  
  
b. Exibe uma mensagem de logout explícita para os usuários, indicando o encerramento confiável de sessões de comunicação autenticadas.  
Guia Adicional: Os recursos de informação aos quais os usuários obtêm acesso via autenticação incluem, por exemplo, estações de trabalho locais, bancos de dados e sites / serviços baseados na Web protegidos por senha. As mensagens de logout para acesso à página da web, por exemplo, podem ser exibidas após o término das sessões autenticadas. No entanto, para alguns tipos de sessões interativas, incluindo, por exemplo, sessões de protocolo de transferência de arquivos (FTP), os sistemas de informações geralmente enviam mensagens de logout como mensagens finais antes de encerrar as sessões.

## AC-13: Supervisão e Revisão - Controle de Acesso (P0)

**Descrição do Controle:**[Retirado: Incorporado no AC-2 e AU-6].

## AC-14: Ações Permitidas Sem Identificação ou Autenticação (P3)

**Descrição do Controle:**A organização:  
  
a. Identifica [Atribuição: ações do usuário definidas pela organização] que pode ser executada no sistema de informações sem identificação ou autenticação consistente com as missões organizacionais / funções de negócios; e  
  
b. Documenta e fornece justificativa de suporte no plano de segurança do sistema de informações, ações do usuário que não exigem identificação ou autenticação.  
  
**Guia Adicional:**Esse controle aborda situações nas quais as organizações determinam que nenhuma identificação ou autenticação é necessária nos sistemas de informações organizacionais. As organizações podem permitir um número limitado de ações do usuário sem identificação ou autenticação, incluindo, por exemplo, quando indivíduos acessam sites públicos ou outros sistemas de informações federais acessíveis ao público, quando indivíduos usam telefones celulares para receber chamadas ou quando fac-símiles são recebidos. As organizações também identificam ações que normalmente requerem identificação ou autenticação, mas podem, sob certas circunstâncias (por exemplo, emergências), permitir que mecanismos de identificação ou autenticação sejam contornados. Tais desvios podem ocorrer, por exemplo, por meio de um comutador físico legível por software que comanda o bypass da funcionalidade de login e é protegido contra o uso acidental ou não monitorado. Esse controle não se aplica a situações em que a identificação e a autenticação já ocorreram e não são repetidas, mas sim a situações em que a identificação e a autenticação ainda não ocorreram. As organizações podem decidir que não há ações do usuário que possam ser executadas nos sistemas de informações organizacionais sem identificação e autenticação e, portanto, os valores das instruções de atribuição podem ser nenhum.  
  
**Melhorias do Controle:**

### AC-14(1): Ações Permitidas Sem Identificação ou Autenticação | Usos Necessários

[Retirado: Incorporado ao AC-14].

## AC-15: Marcação Automatizada (P0)

**Descrição do Controle:**[Retirado: Incorporado em MP-3].

## AC-16: Atributos de Segurança (P0)

**Descrição do Controle:**A organização:  
  
a. Fornece os meios para associar [Atribuição: tipos de atributos de segurança definidos pela organização] com [Atribuição: valores de atributos de segurança definidos pela organização] com informações em armazenamento, em processo e/ou em transmissão;  
  
b. Garante que as associações de atributos de segurança sejam feitas e mantidas com as informações;  
  
c. Estabelece a [Atribuição: atributos de segurança definidos pela organização] permitidos para [Atribuição: sistemas de informações definidas pela organização]; e  
  
d. Determina a [Atribuição atribuída: valores ou intervalos definidos pela organização] para cada um dos atributos de segurança estabelecidos.  
  
**Guia Adicional:**A informação é representada internamente em sistemas de informação usando abstrações conhecidas como estruturas de dados. Estruturas de dados internas podem representar diferentes tipos de entidades, ativas e passivas. Entidades ativas, também conhecidas como assuntos, são normalmente associadas a indivíduos, dispositivos ou processos agindo em nome de indivíduos. As entidades passivas, também conhecidas como objetos, são normalmente associadas a estruturas de dados, como registros, buffers, tabelas, arquivos, pipes entre processos e portas de comunicação. Atributos de segurança, uma forma de metadados, são abstrações representando as propriedades básicas ou características de entidades ativas e passivas com relação à proteção de informações. Esses atributos podem estar associados a entidades ativas (isto é, sujeitos) que têm o potencial de enviar ou receber informações, fazer com que as informações fluam entre objetos ou alterar o estado do sistema de informações. Esses atributos também podem estar associados a entidades passivas (isto é, objetos) que contêm ou recebem informações. A associação de atributos de segurança a assuntos e objetos é chamada de ligação e geralmente inclui a definição do valor do atributo e do tipo de atributo. Atributos de segurança quando vinculados a dados / informações, permitem a aplicação de políticas de segurança de informações para controle de acesso e controle de fluxo de informações, seja através de processos organizacionais ou funções ou mecanismos do sistema de informações. O conteúdo ou os valores atribuídos dos atributos de segurança podem afetar diretamente a capacidade dos indivíduos de acessar informações organizacionais. As organizações podem definir os tipos de atributos necessários para sistemas de informação selecionados para suportar funções de missão / negócios. Existe potencialmente um amplo intervalo de valores que podem ser atribuídos a qualquer atributo de segurança. As marcas de lançamento podem incluir, por exemplo, apenas EUA, NATO ou NOFORN (não liberáveis para cidadãos estrangeiros). Ao especificar intervalos e valores de atributos permitidos, as organizações podem garantir que os valores do atributo de segurança sejam significativos e relevantes. O termo rotulagem de segurança refere-se à associação de atributos de segurança com sujeitos e objetos representados por estruturas internas de dados dentro dos sistemas de informações organizacionais, para permitir a imposição de políticas de segurança da informação baseadas no sistema de informações. Os rótulos de segurança incluem, por exemplo, autorizações de acesso, proteção do ciclo de vida de dados (isto é, criptografia e expiração de dados), nacionalidade, afiliação como contratante e classificação de informações de acordo com os requisitos legais e de conformidade. O termo marcação de segurança refere-se à associação de atributos de segurança com objetos de forma legível, para permitir a imposição de políticas de segurança da informação baseadas em processos organizacionais. O controle base AC-16 representa o requisito para associação de atributos baseada em usuário (marcação). Os aprimoramentos do AC-16 representam requisitos adicionais, incluindo associação de atributos baseada em sistema de informações (rotulagem). Os tipos de atributos incluem, por exemplo, nível de classificação para objetos e nível de autorização (autorização de acesso) para sujeitos. Um exemplo de valor para ambos os tipos de atributos é Top Secret.  
  
**Melhorias do Controle:**

### AC-16(1): Atributos de Segurança | Associação de Atributos Dinâmicos

O sistema de informações associa dinamicamente os atributos de segurança a [Atribuição: objetos e assuntos definidos pela organização] de acordo com [Atribuição: políticas de segurança definidas pela organização] à medida que as informações são criadas e combinadas.  
Guia Adicional: A associação dinâmica de atributos de segurança é apropriada sempre que as características de segurança das informações mudam ao longo do tempo. Os atributos de segurança podem mudar, por exemplo, devido a problemas de agregação de informações (ou seja, as características de segurança de elementos de informações individuais são diferentes dos elementos combinados), alterações nas autorizações de acesso individuais (ou seja, privilégios) e alterações na categoria de segurança das informações.

### AC-16(2): Atributos de Segurança | Alterações de Valor Atribuído por Indivíduos Autorizados

O sistema de informações fornece a indivíduos autorizados (ou processos agindo em nome de indivíduos) a capacidade de definir ou alterar o valor dos atributos de segurança associados.  
Guia Adicional: O conteúdo ou os valores atribuídos dos atributos de segurança podem afetar diretamente a capacidade dos indivíduos de acessar informações organizacionais. Portanto, é importante que os sistemas de informação possam limitar a capacidade de criar ou modificar atributos de segurança para indivíduos autorizados.

### AC-16(3): Atributos de Segurança | Manutenção de Associações Atribuídas por Sistema de Informação

O sistema de informações mantém a associação e a integridade de [Atribuição: atributos de segurança definidos pela organização] a [Atribuição: assuntos e objetos definidos pela organização].  
Guia Adicional: Manter a associação e a integridade dos atributos de segurança para assuntos e objetos com garantia suficiente ajuda a garantir que as associações de atributos possam ser usadas como base para ações de política automatizadas. As ações de política automatizadas incluem, por exemplo, decisões de controle de acesso ou decisões de controle de fluxo de informações.

### AC-16(4): Atributos de Segurança | Associação de Atributos por Indivíduos Autorizados

O sistema de informações suporta a associação de [Atribuição: atributos de segurança definidos pela organização] a [Atribuição: assuntos e objetos definidos pela organização] por indivíduos autorizados (ou processos agindo em nome de indivíduos).  
Guia Adicional: O suporte fornecido pelos sistemas de informação pode variar para incluir: (i) solicitar aos usuários que selecionem atributos de segurança específicos a serem associados a objetos de informação específicos; (ii) empregar mecanismos automatizados para categorizar informações com atributos apropriados, com base em políticas definidas; ou (iii) garantir que a combinação de atributos de segurança selecionados seja válida. As organizações consideram a criação, exclusão ou modificação de atributos de segurança ao definir eventos auditáveis.

### AC-16(5): Atributos de Segurança | Exibição de Atributos para Dispositivos de Saída

O sistema de informações exibe atributos de segurança em formato legível por humanos em cada objeto que o sistema transmite para os dispositivos de saída para identificar [Tarefa: instruções especiais de disseminação, manipulação ou distribuição identificadas pela organização] usando [Tarefa: padrão legível por humanos, identificada pela organização convenções de nomenclatura].  
Guia Adicional: As saídas do sistema de informação incluem, por exemplo, páginas, telas ou equivalente. Os dispositivos de saída do sistema de informação incluem, por exemplo, impressoras e monitores de vídeo em estações de trabalho de computadores, notebooks e assistentes digitais pessoais.

### AC-16(6): Atributos de Segurança | Manutenção da Associação Atribuída por Organização

A organização permite que o pessoal associe e mantenha a associação de [Atribuição: atributos de segurança definidos pela organização] com [Atribuição: objetos e assuntos definidos pela organização] de acordo com [Atribuição: políticas de segurança definidas pela organização].  
Guia Adicional: Esse aprimoramento de controle requer que usuários individuais (em oposição ao sistema de informações) mantenham associações de atributos de segurança com assuntos e objetos.

### AC-16(7): Atributos de Segurança | Interpretação Atributa Consistente

A organização fornece uma interpretação consistente dos atributos de segurança transmitidos entre os componentes do sistema de informações distribuídas.  
Guia Adicional: Para impor políticas de segurança em vários componentes em sistemas de informações distribuídos (por exemplo, sistemas de gerenciamento de banco de dados distribuídos, sistemas baseados em nuvem e arquiteturas orientadas a serviços), as organizações fornecem uma interpretação consistente dos atributos de segurança usados na imposição de acesso e imposição de fluxo decisões. As organizações estabelecem acordos e processos para garantir que todos os componentes do sistema de informações distribuídas implementem atributos de segurança com interpretações consistentes em ações automatizadas de imposição de acesso / fluxo.

### AC-16(8): Atributos de Segurança | Técnicas/Tecnologias de Associação

O sistema de informação implementa [Atribuição: técnicas ou tecnologias definidas pela organização] com [Atribuição: nível de garantia definido pela organização] na associação de atributos de segurança às informações.  
Guia Adicional: A associação (ou seja, vinculação) de atributos de segurança às informações nos sistemas de informação é de importância significativa no que se refere à realização de ações automatizadas de imposição de acesso e imposição de fluxo. A associação desses atributos de segurança pode ser realizada com tecnologias / técnicas que fornecem diferentes níveis de garantia. Por exemplo, os sistemas de informação podem vincular criptograficamente atributos de segurança a informações usando assinaturas digitais com as chaves criptográficas de suporte protegidas por dispositivos de hardware (algumas vezes conhecidas como raízes de confiança de hardware).

### AC-16(9): Atributos de Segurança | Atribuição de Atribuição

A organização garante que os atributos de segurança associados às informações sejam atribuídos novamente apenas por meio de mecanismos de nova classificação validados usando [Atribuição: técnicas ou procedimentos definidos pela organização].  
Guia Adicional: Mecanismos de reclassificação validados são empregados pelas organizações para fornecer os níveis necessários de garantia para atividades de revalidação de atributos de segurança. A validação é facilitada, garantindo que os mecanismos de nova classificação sejam de propósito único e de função limitada. Como as resignações de atributos de segurança podem afetar as ações de imposição de políticas de segurança (por exemplo, decisões de imposição de acesso / fluxo), é necessário o uso de mecanismos confiáveis de nova classificação para garantir que esses mecanismos sejam executados em um modo de operação consistente / correto.

### AC-16(10): Atributos de Segurança | Configuração Atribuída por Indivíduos Autorizados

O sistema de informações fornece às pessoas autorizadas a capacidade de definir ou alterar o tipo e o valor dos atributos de segurança disponíveis para associação com sujeitos e objetos.  
Guia Adicional: O conteúdo ou os valores atribuídos dos atributos de segurança podem afetar diretamente a capacidade dos indivíduos de acessar informações organizacionais. Portanto, é importante que os sistemas de informações possam limitar a capacidade de criar ou modificar atributos de segurança apenas para indivíduos autorizados.

## AC-17: Acesso Remoto (P1)

**Descrição do Controle:**A organização:  
  
a. Estabelece e documenta restrições de uso, requisitos de configuração / conexão e orientação de implementação para cada tipo de acesso remoto permitido; e  
  
b. Autoriza o acesso remoto ao sistema de informações antes de permitir tais conexões.  
  
**Guia Adicional:**Acesso remoto é o acesso aos sistemas de informações organizacionais pelos usuários (ou processos agindo em nome dos usuários) que se comunicam através de redes externas (por exemplo, a Internet). Os métodos de acesso remoto incluem, por exemplo, discagem, banda larga e sem fio. As organizações geralmente empregam redes privadas virtuais (VPNs) criptografadas para aprimorar a confidencialidade e a integridade em conexões remotas. O uso de VPNs criptografadas não torna o acesso não remoto; no entanto, o uso de VPNs, quando adequadamente provisionados com controles de segurança apropriados (por exemplo, empregando técnicas de criptografia apropriadas para confidencialidade e proteção de integridade) pode fornecer garantia suficiente para a organização de que pode tratar efetivamente tais conexões como redes internas. Ainda assim, as conexões VPN atravessam redes externas e a VPN criptografada não aprimora a disponibilidade de conexões remotas. Além disso, as VPNs com túneis criptografados podem afetar a capacidade organizacional de monitorar adequadamente o tráfego de comunicações da rede em busca de códigos maliciosos. Os controles de acesso remoto se aplicam a sistemas de informação que não sejam servidores públicos da Web ou sistemas projetados para acesso público. Esse controle aborda a autorização antes de permitir acesso remoto sem especificar os formatos para tal autorização. Embora as organizações possam usar contratos de segurança de interconexão para autorizar conexões de acesso remoto, esses contratos não são exigidos por esse controle. A imposição de restrições de acesso para conexões remotas é abordada no AC-3.  
  
**Melhorias do Controle:**

### AC-17(1): Acesso Remoto | Monitoramento/Controle Automatizado

O sistema de informações monitora e controla os métodos de acesso remoto.  
Guia Adicional: O monitoramento e controle automatizados das sessões de acesso remoto permitem que as organizações detectem ataques cibernéticos e também garantam a conformidade contínua com as políticas de acesso remoto, auditando as atividades de conexão de usuários remotos em uma variedade de componentes do sistema de informações (por exemplo, servidores, estações de trabalho, notebooks, smartphones, e comprimidos).

### AC-17(2): Acesso Remoto | Proteção da Confidencialidade/Integridade Usando Criptografia

O sistema de informações implementa mecanismos criptográficos para proteger a confidencialidade e a integridade das sessões de acesso remoto.  
Guia Adicional: O nível de criptografia do mecanismo é selecionado com base na categorização de segurança das informações.

### AC-17(3): Acesso Remoto | Gestão dos Pontos de Controle de Acesso

O sistema de informações roteia todos os acessos remotos através dos pontos de controle de acesso gerenciado pela rede [Atribuição: número definido pela organização].  
Guia Adicional: Limitar o número de pontos de controle de acesso para acessos remotos reduz a superfície de ataque das organizações. As organizações consideram os requisitos da iniciativa Trusted Internet Connections (TIC) para conexões de rede externas.

### AC-17(4): Acesso Remoto | Comandos/Acesso Privilegiados

A organização:  
  
a. Autoriza a execução de comandos privilegiados e o acesso a informações relevantes à segurança via acesso remoto apenas para [Atribuição: necessidades definidas pela organização]; e  
  
b. Documenta a justificativa para esse acesso no plano de segurança do sistema de informações.

### AC-17(5): Acesso Remoto | Monitoramento de Conexões Não Autorizadas

[Retirado: Incorporado no SI-4].

### AC-17(6): Acesso Remoto | Proteção da Informação

A organização garante que os usuários protejam as informações sobre os mecanismos de acesso remoto contra uso e divulgação não autorizados.

### AC-17(7): Acesso Remoto | Proteção Adicional para Acesso à Função de Segurança

[Retirado: Incorporado ao AC-3 (10)].

### AC-17(8): Acesso Remoto | Desativar Protocolos de Rede Não Segura

[Retirado: Incorporado ao CM-7].

### AC-17(9): Acesso Remoto | Desconectar/Desativar Acesso

A organização oferece a capacidade de desconectar ou desativar rapidamente o acesso remoto ao sistema de informações dentro de [Atribuição: período definido pela organização].  
Guia Adicional: Esse aprimoramento de controle exige que as organizações tenham a capacidade de desconectar rapidamente os usuários atuais que acessam remotamente o sistema de informações e/ou desabilitar o acesso remoto adicional. A velocidade de desconexão ou desativação varia de acordo com a criticidade das funções de missões / negócios e a necessidade de eliminar o acesso remoto imediato ou futuro aos sistemas de informações organizacionais.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-46 | https://csrc.nist.gov/publications/search?keywords-lg=800-46 |
| Publicação Especial NIST 800-77 | https://csrc.nist.gov/publications/search?keywords-lg=800-77 |
| Publicação Especial NIST 800-113 | https://csrc.nist.gov/publications/search?keywords-lg=800-113 |
| Publicação Especial NIST 800-114 | https://csrc.nist.gov/publications/search?keywords-lg=800-114 |
| Publicação Especial NIST 800-121 | https://csrc.nist.gov/publications/search?keywords-lg=800-121 |

## AC-18: Acesso Sem Fio (P1)

**Descrição do Controle:**A organização:  
  
a. Estabelece restrições de uso, requisitos de configuração / conexão e diretrizes de implementação para acesso sem fio; e  
  
b. Autoriza o acesso sem fio ao sistema de informações antes de permitir tais conexões.  
  
**Guia Adicional:**As tecnologias sem fio incluem, por exemplo, micro-ondas, rádio de pacote (UHF / VHF), 802.11x e Bluetooth. As redes sem fio usam protocolos de autenticação (por exemplo, EAP / TLS, PEAP), que fornecem proteção de credencial e autenticação mútua.  
  
**Melhorias do Controle:**

### AC-18(1): Acesso Sem Fio | Autenticação e Criptografia

O sistema de informações protege o acesso sem fio ao sistema usando a autenticação de [Seleção (um ou mais): usuários; dispositivos] e criptografia.

### AC-18(2): Acesso Sem Fio | Monitorando Ligações Não Autorizadas

[Retirado: Incorporado no SI-4].

### AC-18(3): Acesso Sem Fio | Desativar Rede Sem Fios

A organização desativa, quando não se destina ao uso, os recursos de rede sem fio incorporados internamente nos componentes do sistema de informações antes da emissão e implantação.

### AC-18(4): Acesso Sem Fio | Configurações Restritas pelos Usuários

A organização identifica e autoriza explicitamente os usuários com permissão para configurar independentemente os recursos de rede sem fio.  
Guia Adicional: As autorizações organizacionais para permitir que usuários selecionados configurem o recurso de rede sem fio são aplicadas em parte pelos mecanismos de imposição de acesso empregados nos sistemas de informações organizacionais.

### AC-18(5): Acesso Sem Fio | Níveis de Energia da Antena/Transmissão

A organização seleciona antenas de rádio e calibra os níveis de potência de transmissão para reduzir a probabilidade de que sinais utilizáveis possam ser recebidos fora dos limites controlados pela organização.  
Guia Adicional: As ações que podem ser tomadas pelas organizações para limitar o uso não autorizado de comunicações sem fio fora dos limites controlados pela organização incluem, por exemplo: (i) reduzir o poder das transmissões sem fio para que as transmissões tenham menos probabilidade de emitir um sinal que possa ser usado por adversários fora do perímetro físico das organizações; (ii) empregar medidas como a TEMPEST para controlar as emanações sem fio; e (iii) usando antenas direcionais / formador de feixe que reduzem a probabilidade de que receptores não desejados sejam capazes de interceptar sinais. Antes de tomar essas ações, as organizações podem realizar pesquisas sem fio periódicas para entender o perfil de radiofrequência dos sistemas de informações organizacionais, bem como outros sistemas que possam estar operando na área.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-48 | https://csrc.nist.gov/publications/search?keywords-lg=800-48 |
| Publicação Especial NIST 800-94 | https://csrc.nist.gov/publications/search?keywords-lg=800-94 |
| Publicação Especial NIST 800-97 | https://csrc.nist.gov/publications/search?keywords-lg=800-97 |

## AC-19: Controle de Acesso para Dispositivos Móveis (P1)

**Descrição do Controle:**A organização:  
  
a. Estabelece restrições de uso, requisitos de configuração, requisitos de conexão e orientação de implementação para dispositivos móveis controlados pela organização; e  
  
b. Autoriza a conexão de dispositivos móveis a sistemas de informações organizacionais.  
  
**Guia Adicional:**Um dispositivo móvel é um dispositivo de computação que: (i) possui um pequeno fator de forma que pode ser facilmente transportado por um único indivíduo; (ii) é projetado para operar sem uma conexão física (por exemplo, transmitir ou receber informações sem fio); (iii) possui armazenamento de dados local, não removível ou removível; e (iv) inclui uma fonte de energia independente. Os dispositivos móveis também podem incluir recursos de comunicação de voz, sensores integrados que permitem que o dispositivo capture informações e/ou recursos internos para sincronizar dados locais com locais remotos. Exemplos incluem telefones inteligentes, leitores eletrônicos e tablets. Dispositivos móveis são normalmente associados a um único indivíduo e o dispositivo geralmente está próximo ao indivíduo; no entanto, o grau de proximidade pode variar dependendo do fator de forma e do tamanho do dispositivo. A capacidade de processamento, armazenamento e transmissão do dispositivo móvel pode ser comparável ou meramente um subconjunto de sistemas de desktop, dependendo da natureza e finalidade do dispositivo. Devido à grande variedade de dispositivos móveis com diferentes características e capacidades técnicas, as restrições organizacionais podem variar para as diferentes classes / tipos desses dispositivos. Restrições de uso e orientações específicas de implementação para dispositivos móveis incluem, por exemplo, gerenciamento de configuração, identificação e autenticação de dispositivos, implementação de software de proteção obrigatório (por exemplo, detecção de código malicioso, firewall), verificação de código malicioso, atualização de software antivírus, verificação de atualizações e patches críticos de software, conduzindo verificações de integridade do sistema operacional primário (e possivelmente de outro software residente) e desabilitando hardware desnecessário (por exemplo, sem fio, infravermelho). As organizações são alertadas de que a necessidade de fornecer segurança adequada para dispositivos móveis vai além dos requisitos deste controle. Muitas salvaguardas e contramedidas para dispositivos móveis são refletidas em outros controles de segurança no catálogo alocado nas linhas de base de controle inicial como pontos de partida para o desenvolvimento de planos e sobreposições de segurança usando o processo de adaptação. Também pode haver algum grau de sobreposição nos requisitos articulados pelos controles de segurança nas diferentes famílias de controles. O AC-20 aborda dispositivos móveis que não são controlados pela organização.  
  
**Melhorias do Controle:**

### AC-19(1): Controle de Acesso para Dispositivos Móveis | Utilização de Dispositivo Portátil de Armazenamento

[Retirado: Incorporado ao MP-7].

### AC-19(2): Controle de Acesso para Dispositivos Móveis | Utilização de Dispositivo Portátil de Armazenamento Pessoal

[Retirado: Incorporado ao MP-7].

### AC-19(3): Controle de Acesso para Dispositivos Móveis | Utilização de Dispositivo Portátil de Armazenamento, Sem Proprietário Identificável

[Retirado: Incorporado ao MP-7].

### AC-19(4): Controle de Acesso para Dispositivos Móveis | Restrições à Informação Confidencial

A organização:  
  
a. Proíbe o uso de dispositivos móveis não classificados em instalações que contêm sistemas de informação que processam, armazenam ou transmitem informações classificadas, a menos que especificamente permitido pelo autorizador; e  
  
b. Aplica as seguintes restrições às pessoas autorizadas pelo funcionário autorizador a usar dispositivos móveis não classificados em instalações que contêm sistemas de informações que processam, armazenam ou transmitem informações classificadas:  
  
c. Restringe a conexão de dispositivos móveis classificados a sistemas de informações classificadas de acordo com [Atribuição: políticas de segurança definidas pela organização].

### AC-19(5): Controle de Acesso para Dispositivos Móveis | Criptografia Completa do Dispositivo/Container

A organização emprega [Seleção: criptografia de dispositivo completo; criptografia de contêiner] para proteger a confidencialidade e a integridade das informações em [Atribuição: dispositivos móveis definidos pela organização].  
Guia Adicional: A criptografia baseada em contêiner fornece uma abordagem mais refinada à criptografia de dados / informações em dispositivos móveis, incluindo, por exemplo, criptografia de estruturas de dados selecionadas, como arquivos, registros ou campos.

**Referências:**

|  |  |
| --- | --- |
| OMB Memorando 06-16 | https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2006/m06-16.pdf |
| Publicação Especial NIST 800-114 | https://csrc.nist.gov/publications/search?keywords-lg=800-114 |
| Publicação Especial NIST 800-124 | https://csrc.nist.gov/publications/search?keywords-lg=800-124 |
| Publicação Especial NIST 800-164 | https://csrc.nist.gov/publications/search?keywords-lg=800-164 |

## AC-20: Utilização de Sistemas Externos (P1)

**Descrição do Controle:**A organização estabelece termos e condições, consistentes com quaisquer relacionamentos de confiança estabelecidos com outras organizações que possuem, operam e/ou mantêm sistemas de informações externos, permitindo que indivíduos autorizados:  
  
a. Acessar o sistema de informação a partir de sistemas de informação externos; e  
  
b. Processe, armazene ou transmita informações controladas pela organização usando sistemas de informação externos.  
  
**Guia Adicional:**Sistemas de informação externos são sistemas de informação ou componentes de sistemas de informação que estão fora do limite de autorização estabelecido pelas organizações e para as quais as organizações normalmente não têm supervisão direta e autoridade sobre a aplicação dos controles de segurança necessários ou a avaliação da eficácia do controle. Os sistemas de informações externas incluem, por exemplo: (i) sistemas / dispositivos de informações de propriedade pessoal (por exemplo, notebooks, smartphones, tablets, assistentes digitais pessoais); (ii) dispositivos de computação e comunicações de propriedade privada residentes em instalações comerciais ou públicas (por exemplo, hotéis, estações de trem, centros de convenções, shopping centers ou aeroportos); (iii) sistemas de informação pertencentes ou controlados por organizações governamentais não federais; e (iv) sistemas federais de informação que não pertencem, são operados ou estão sob a supervisão e autoridade diretas das organizações. Esse controle também aborda o uso de sistemas de informações externas para processamento, armazenamento ou transmissão de informações organizacionais, incluindo, por exemplo, o acesso a serviços em nuvem (por exemplo, infraestrutura como um serviço, plataforma como um serviço ou software como serviço) de sistemas de informação organizacional. Para alguns sistemas de informação externos (ou seja, sistemas de informação operados por outras agências federais, incluindo organizações subordinadas a essas agências), as relações de confiança estabelecidas entre essas organizações e a organização de origem podem ser tais que não são necessários termos e condições explícitos. Os sistemas de informação dentro dessas organizações não seriam considerados externos. Essas situações ocorrem quando, por exemplo, existem acordos de compartilhamento / confiança preexistentes (implícitos ou explícitos) estabelecidos entre agências federais ou organizações subordinadas a essas agências, ou quando tais acordos de confiança são especificados por leis aplicáveis, ordens executivas, diretivas ou políticas. Os indivíduos autorizados incluem, por exemplo, pessoal da organização, contratados ou outros indivíduos com acesso autorizado aos sistemas de informações organizacionais e sobre quais organizações têm autoridade para impor regras de comportamento com relação ao acesso ao sistema. Restrições que as organizações impõem aos indivíduos autorizados não precisam ser uniformes, pois essas restrições podem variar dependendo das relações de confiança entre as organizações. Portanto, as organizações podem optar por impor restrições de segurança diferentes aos contratados e aos governos estaduais, locais ou tribais. Esse controle não se aplica ao uso de sistemas de informação externos para acessar interfaces públicas para sistemas de informações organizacionais (por exemplo, indivíduos acessando informações federais através de www.usa.gov). As organizações estabelecem termos e condições para o uso de sistemas de informações externos, de acordo com as políticas e procedimentos de segurança organizacional. Os termos e condições tratam no mínimo: tipos de aplicativos que podem ser acessados em sistemas de informações organizacionais a partir de sistemas de informações externos; e a categoria de segurança mais alta que pode ser processada, armazenada ou transmitida em sistemas de informações externos. Se os termos e condições com os proprietários de sistemas de informação externos não puderem ser estabelecidos, as organizações podem impor restrições ao pessoal organizacional usando esses sistemas externos.  
  
**Melhorias do Controle:**

### AC-20(1): Utilização de Sistemas Externos | Limites de Uso Autorizado

A organização permite que indivíduos autorizados usem um sistema de informações externo para acessar o sistema de informações ou processar, armazenar ou transmitir informações controladas pela organização somente quando a organização:  
  
a. Verifica a implementação dos controles de segurança necessários no sistema externo, conforme especificado na política de segurança da informação e no plano de segurança da organização; ou  
  
b. Mantém contratos de conexão ou processamento aprovados do sistema de informações com a entidade organizacional que hospeda o sistema de informações externo.  
Guia Adicional: Esse aprimoramento de controle reconhece que há circunstâncias em que indivíduos que usam sistemas de informação externos (por exemplo, contratados, parceiros de coalizão) precisam acessar sistemas de informações organizacionais. Nessas situações, as organizações precisam ter confiança de que os sistemas de informações externos contêm as salvaguardas de segurança necessárias (isto é, controles de segurança), para não comprometer, danificar ou prejudicar os sistemas de informações organizacionais. A verificação de que os controles de segurança exigidos foram implementados pode ser obtida, por exemplo, por avaliações independentes de terceiros, atestados ou outros meios, dependendo do nível de confiança exigido pelas organizações.

### AC-20(2): Utilização de Sistemas Externos | Dispositivos Portáteis de Armazenamento

A organização [Seleção: restringe; proíbe] o uso de dispositivos de armazenamento portáteis controlados pela organização por indivíduos autorizados em sistemas de informação externos.  
Guia Adicional: Os limites do uso de dispositivos de armazenamento portáteis controlados pela organização em sistemas de informações externos incluem, por exemplo, proibição completa do uso de tais dispositivos ou restrições sobre como os dispositivos podem ser usados e sob quais condições os dispositivos podem ser utilizados.

### AC-20(3): Utilização de Sistemas Externos | Sistemas / Componentes / Dispositivos Não Organizacionais

A organização [Seleção: restringe; proíbe] o uso de sistemas, componentes ou dispositivos de informações de propriedade não organizacional para processar, armazenar ou transmitir informações organizacionais.  
Guia Adicional: Dispositivos de propriedade não organizacional incluem dispositivos de outras organizações (por exemplo, agências federais / estaduais, prestadores de serviços) e dispositivos de propriedade pessoal. Existem riscos no uso de dispositivos de propriedade não organizacional. Em alguns casos, o risco é suficientemente alto para proibir esse uso. Em outros casos, pode ser tal que o uso de dispositivos de propriedade não organizacional seja permitido, mas restrito de alguma forma. As restrições incluem, por exemplo: (i) exigir a implementação de controles de segurança aprovados pela organização antes da autorização de tais conexões; (ii) limitar o acesso a certos tipos de informações, serviços ou aplicativos; (iii) usando técnicas de virtualização para limitar as atividades de processamento e armazenamento a servidores ou outros componentes do sistema provisionados pela organização; e (iv) concordar com os termos e condições de uso. Para dispositivos de propriedade pessoal, as organizações consultam o Escritório do Conselho Geral sobre questões legais associadas ao uso de tais dispositivos em ambientes operacionais, incluindo, por exemplo, requisitos para a realização de análises forenses durante investigações após um incidente.

### AC-20(4): Utilização de Sistemas Externos | Dispositivos de Armazenamento Acessíveis por Rede

A organização proíbe o uso de [Atribuição: dispositivos de armazenamento acessíveis em rede definidos pela organização] em sistemas de informações externos.  
Guia Adicional: Os dispositivos de armazenamento acessíveis em rede em sistemas de informações externos incluem, por exemplo, dispositivos de armazenamento online em sistemas públicos, híbridos ou baseados em nuvem da comunidade.

**Referências:**

|  |  |
| --- | --- |
| Publicações de Normas Federais de Processamento de Informações N.199 | http://csrc.nist.gov/publications/PubsFIPS.html#199 |

## AC-21: Compartilhamento de Informações (P2)

**Descrição do Controle:**A organização:  
  
a. Facilita o compartilhamento de informações, permitindo que usuários autorizados determinem se as autorizações de acesso atribuídas ao parceiro de compartilhamento correspondem às restrições de acesso às informações para [Atribuição: circunstâncias de compartilhamento de informações definidas pela organização em que a discrição do usuário é necessária]; e  
  
b. Emprega [Atribuição: mecanismos automatizados definidos pela organização ou processos manuais] para ajudar os usuários a tomar decisões de compartilhamento / colaboração de informações.  
  
**Guia Adicional:**Esse controle aplica-se a informações que podem ser restritas de alguma maneira (por exemplo, informações médicas privilegiadas, informações sensíveis a contratos, informações proprietárias, informações de identificação pessoal, informações classificadas relacionadas a programas ou compartimentos especiais de acesso) com base em alguma determinação formal ou administrativa. Dependendo das circunstâncias específicas de compartilhamento de informações, os parceiros de compartilhamento podem ser definidos no nível individual, de grupo ou organizacional. As informações podem ser definidas por conteúdo, tipo, categoria de segurança ou programa / compartimento de acesso especial.  
  
**Melhorias do Controle:**

### AC-21(1): Compartilhamento de Informações | Automatização do Apoio à Decisão

O sistema de informações impõe decisões de compartilhamento de informações por usuários autorizados, com base nas autorizações de acesso de parceiros de compartilhamento e restrições de acesso às informações a serem compartilhadas.

### AC-21(2): Compartilhamento de Informações | Pesquisa e Recuperação de Informação

O sistema de informações implementa serviços de busca e recuperação de informações que impõem [Atribuição: restrições de compartilhamento de informações definidas pela organização].

## AC-22: Conteúdo Público Acessível (P3)

**Descrição do Controle:**A organização:  
  
a. Designa indivíduos autorizados a publicar informações em um sistema de informações acessível ao público;  
  
b. Treina indivíduos autorizados para garantir que informações publicamente acessíveis não contenham informações não públicas;  
  
c. Revê o conteúdo proposto de informação antes de publicar no sistema de informação de acesso público para garantir que as informações não públicas não sejam incluídas; e  
  
d. Revisa o conteúdo do sistema de informações de acesso público para informações não públicas [Atribuição: frequência definida pela organização] e remove essas informações, se descobertas.  
  
**Guia Adicional:**De acordo com as leis federais, ordens executivas, diretivas, políticas, regulamentos, normas e/ou orientações, o público em geral não tem acesso autorizado a informações não públicas (por exemplo, informações protegidas pelo Privacy Act e informações proprietárias). Esse controle aborda sistemas de informação que são controlados pela organização e acessíveis ao público em geral, normalmente sem identificação ou autenticação. A publicação de informações sobre sistemas de informações não pertencentes à organização é coberta pela política organizacional.

## AC-23: Proteção contra Mineração de Dados (P0)

**Descrição do Controle:**A organização emprega [Atribuição: técnicas de prevenção e detecção de mineração de dados definida pela organização] para [Atribuição: objetos de armazenamento de dados definidos pela organização] para detectar e proteger adequadamente a mineração de dados.  
  
**Guia Adicional:**Objetos de armazenamento de dados incluem, por exemplo, bancos de dados, registros de banco de dados e campos de banco de dados. As técnicas de prevenção e detecção de mineração de dados incluem, por exemplo: (i) limitação dos tipos de respostas fornecidas às consultas ao banco de dados; (ii) limitar o número / frequência de consultas ao banco de dados para aumentar o fator de trabalho necessário para determinar o conteúdo desses bancos de dados; e (iii) notificar o pessoal da organização quando ocorrem consultas ou acessos atípicos ao banco de dados. Esse controle se concentra na proteção das informações organizacionais da mineração de dados enquanto essas informações residem nos armazenamentos de dados organizacionais. Em contraste, a AU-13 se concentra no monitoramento de informações organizacionais que podem ter sido extraídas ou obtidas de outros armazenamentos de dados e agora estão disponíveis como informações de código aberto residindo em sites externos, por exemplo, através de redes sociais ou sites de mídia social.

## AC-24: Decisões sobre Controle de Acesso (P0)

**Descrição do Controle:**A organização estabelece procedimentos para garantir que [Atribuição: decisões de controle de acesso definidas pela organização] sejam aplicadas a cada solicitação de acesso antes da aplicação do acesso.  
  
**Guia Adicional:**As decisões de controle de acesso (também conhecidas como decisões de autorização) ocorrem quando as informações de autorização são aplicadas a acessos específicos. Em contraste, a imposição de acesso ocorre quando os sistemas de informação aplicam as decisões de controle de acesso. Embora seja muito comum ter decisões de controle de acesso e aplicação de acesso implementadas pela mesma entidade, ela não é necessária e nem sempre é uma opção de implementação ideal. Para algumas arquiteturas e sistemas de informações distribuídas, diferentes entidades podem executar decisões de controle de acesso e acesso à aplicação.  
  
**Melhorias do Controle:**

### AC-24(1): Decisões sobre Controle de Acesso | Transmitir Informações de Autorização de Acesso

O sistema de informação transmite [Atribuição: informações de autorização de acesso definido pela organização] usando [Atribuição: salvaguardas de segurança definidas pela organização] para [Atribuição: sistemas de informação definidos pela organização] que impõem decisões de controle de acesso.  
Guia Adicional: Em sistemas de informação distribuídos, processos de autorização e decisões de controle de acesso podem ocorrer em partes separadas dos sistemas. Nesses casos, as informações de autorização são transmitidas com segurança, para que decisões oportunas de controle de acesso possam ser aplicadas nos locais apropriados. Para dar suporte às decisões de controle de acesso, pode ser necessário transmitir como parte das informações de autorização de acesso, suportando atributos de segurança. Isso se deve ao fato de que em sistemas de informação distribuídos, existem várias decisões de controle de acesso que precisam ser tomadas e diferentes entidades (por exemplo, serviços) tomam essas decisões de maneira serial, cada uma exigindo alguns atributos de segurança para tomar as decisões. A proteção das informações de autorização de acesso (ou seja, decisões de controle de acesso) garante que essas informações não possam ser alteradas, falsificadas ou comprometidas durante a transmissão.

### AC-24(2): Decisões sobre Controle de Acesso | Nenhuma Identidade de Usuário ou Processo

O sistema de informações impõe decisões de controle de acesso com base em [Atribuição: atributos de segurança definidos pela organização] que não incluem a identidade do usuário ou processo agindo em nome do usuário.  
Guia Adicional: Em certas situações, é importante que as decisões de controle de acesso possam ser tomadas sem informações sobre a identidade dos usuários que emitem as solicitações. Geralmente, são casos em que a preservação da privacidade individual é de suma importância. Em outras situações, as informações de identificação do usuário simplesmente não são necessárias para as decisões de controle de acesso e, especialmente no caso de sistemas de informações distribuídos, transmitir essas informações com o grau de garantia necessário pode ser muito caro ou difícil de realizar.

## AC-25: Monitor de Referência (P0)

**Descrição do Controle:**O sistema de informações implementa um monitor de referência para [Atribuição: políticas de controle de acesso definidas pela organização] que é à prova de violações, sempre invocada e pequena o suficiente para ser sujeita a análise e teste, cuja integridade pode ser garantida.  
  
**Guia Adicional:**A informação é representada internamente em sistemas de informação usando abstrações conhecidas como estruturas de dados. Estruturas de dados internas podem representar diferentes tipos de entidades, ativas e passivas. Entidades ativas, também conhecidas como assuntos, são normalmente associadas a indivíduos, dispositivos ou processos agindo em nome de indivíduos. As entidades passivas, também conhecidas como objetos, são normalmente associadas a estruturas de dados, como registros, buffers, tabelas, arquivos, pipes entre processos e portas de comunicação. Os monitores de referência normalmente aplicam políticas de controle de acesso obrigatório - um tipo de controle de acesso que restringe o acesso a objetos com base na identidade dos assuntos ou grupos aos quais os assuntos pertencem. Os controles de acesso são obrigatórios porque os sujeitos com certos privilégios (isto é, permissões de acesso) são impedidos de passar esses privilégios para quaisquer outros assuntos, direta ou indiretamente - ou seja, o sistema de informações aplica rigorosamente a política de controle de acesso com base no conjunto de regras estabelecido pela política. A propriedade à prova de violação do monitor de referência impede que os adversários comprometam o funcionamento do mecanismo. A propriedade sempre invocada impede que os adversários ignorem o mecanismo e, portanto, violem a política de segurança. A propriedade smallness ajuda a garantir a integridade na análise e teste do mecanismo para detectar deficiências ou deficiências (isto é, falhas latentes) que impediriam a aplicação da política de segurança.

# AU - Auditoria e Responsabilidade

## AU-1: Política e Procedimentos de Auditoria e Responsabilidade (P1)

**Descrição do Controle:**A organização:  
  
a. Desenvolve, documenta e dissemina para [Atribuição: pessoal ou funções definidos pela organização]:  
  
1. Uma política de auditoria e prestação de contas que trata de propósito, escopo, funções, responsabilidades, comprometimento de gerenciamento, coordenação entre entidades organizacionais e conformidade; e  
  
2. Procedimentos para facilitar a implementação da política de auditoria e prestação de contas e controles associados de auditoria e prestação de contas; e  
  
b. Revisa e atualiza a atual:  
  
1. Política de auditoria e prestação de contas [Atribuição: frequência definida pela organização]; e  
  
2. Procedimentos de auditoria e prestação de contas [Atribuição: frequência definida pela organização].  
  
**Guia Adicional:**Este controle aborda o estabelecimento de políticas e procedimentos para a implementação efetiva de controles de segurança selecionados e melhorias de controle na família AU. As políticas e procedimentos refletem as leis federais aplicáveis, ordens executivas, diretivas, regulamentos, políticas, normas e diretrizes. Políticas e procedimentos do programa de segurança no nível da organização podem tornar desnecessária a necessidade de políticas e procedimentos específicos do sistema. A política pode ser incluída como parte da política geral de segurança da informação para organizações ou, inversamente, pode ser representada por múltiplas políticas refletindo a natureza complexa de certas organizações. Os procedimentos podem ser estabelecidos para o programa de segurança em geral e para sistemas de informação específicos, se necessário. A estratégia de gerenciamento de risco organizacional é um fator chave no estabelecimento de políticas e procedimentos.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-12 | https://csrc.nist.gov/publications/search?keywords-lg=800-12 |
| Publicação Especial NIST 800-100 | https://csrc.nist.gov/publications/search?keywords-lg=800-100 |

## AU-2: Eventos de Auditoria (P1)

**Descrição do Controle:**A organização:  
  
a. Determina que o sistema de informação é capaz de auditar os seguintes eventos: [Atribuição: eventos auditáveis definidos pela organização];  
  
b. Coordena a função de auditoria de segurança com outras entidades organizacionais que exigem informações relacionadas à auditoria para aprimorar o suporte mútuo e ajudar a orientar a seleção de eventos auditáveis;  
  
c. Fornece uma justificativa para o motivo pelo qual os eventos auditáveis são considerados adequados para apoiar investigações após o fato de incidentes de segurança; e  
  
d. Determina que os seguintes eventos devem ser auditados dentro do sistema de informação: [Atribuição: eventos auditados definidos pela organização (o subconjunto dos eventos auditáveis definidos em AU-2 a.) Juntamente com a frequência de (ou situação que exige) auditoria para cada evento identificado].  
  
**Guia Adicional:**Um evento é qualquer ocorrência observável em um sistema de informações organizacionais. As organizações identificam os eventos de auditoria como os eventos que são significativos e relevantes para a segurança dos sistemas de informação e os ambientes em que esses sistemas operam, a fim de atender às necessidades de auditoria específicas e contínuas. Os eventos de auditoria podem incluir, por exemplo, alterações de senha, logins com falha ou falhas de acesso relacionadas a sistemas de informações, uso de privilégios administrativos, uso de credenciais de PIV ou uso de credenciais de terceiros. Ao determinar o conjunto de eventos auditáveis, as organizações consideram a auditoria apropriada para cada um dos controles de segurança a serem implementados. Para equilibrar os requisitos de auditoria com outras necessidades do sistema de informações, esse controle também requer a identificação do subconjunto de eventos auditáveis que são auditados em um determinado momento. Por exemplo, as organizações podem determinar que os sistemas de informação devem ter a capacidade de registrar todos os acessos a arquivos bem-sucedidos e malsucedidos, mas não ativar essa capacidade, exceto em circunstâncias específicas, devido à sobrecarga potencial no desempenho do sistema. Os requisitos de auditoria, incluindo a necessidade de eventos auditáveis, podem ser referenciados em outros controles de segurança e aprimoramentos de controle. As organizações também incluem eventos auditáveis que são exigidos pelas leis federais aplicáveis, ordens executivas, diretivas, políticas, regulamentos e normas. Os registros de auditoria podem ser gerados em vários níveis de abstração, inclusive no nível do pacote, à medida que as informações percorrem a rede. Selecionar o nível apropriado de abstração é um aspecto crítico de um recurso de auditoria e pode facilitar a identificação de causas-raiz para problemas. As organizações consideram na definição de eventos auditáveis, a auditoria necessária para cobrir eventos relacionados, como as etapas em processos distribuídos, baseados em transações (por exemplo, processos distribuídos em várias organizações) e ações que ocorrem em arquiteturas orientadas a serviços.  
  
**Melhorias do Controle:**

### AU-2(1): Eventos de Auditoria | Compilação de Registros de Auditoria de Várias Fontes

[Retirado: Incorporado na AU-12].

### AU-2(2): Eventos de Auditoria | Seleção de Eventos de Auditoria Por Componente

[Retirado: Incorporado na AU-12].

### AU-2(3): Eventos de Auditoria | Revisões E Atualizações

A organização revisa e atualiza os eventos auditados [Atribuição: frequência definida pela organização].  
Guia Adicional: Com o tempo, os eventos que as organizações acreditam que devem ser auditados podem mudar. É necessário revisar e atualizar o conjunto de eventos auditados periodicamente para garantir que o conjunto atual ainda seja necessário e suficiente.

### AU-2(4): Eventos de Auditoria | Funções Privilegiadas

[Retirado: Incorporado ao AC-6 (9)].

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-92 | https://csrc.nist.gov/publications/search?keywords-lg=800-92 |
| FICAM: Identidade Federal, Credencial e Gerenciamento de Acesso | http://idmanagement.gov |

## AU-3: Conteúdo dos Registros de Auditoria (P1)

**Descrição do Controle:**O sistema de informações gera registros de auditoria contendo informações que estabelecem que tipo de evento ocorreu, quando ocorreu o evento, onde ocorreu o evento, a origem do evento, o resultado do evento e a identidade de quaisquer indivíduos ou assuntos associados ao evento.  
  
**Guia Adicional:**O conteúdo do registro de auditoria que pode ser necessário para satisfazer os requisitos desse controle inclui, por exemplo, carimbos de data e hora, endereços de origem e destino, identificadores de usuário / processo, descrições de eventos, indicações de sucesso / falha, nomes de arquivos envolvidos e controle de acesso ou controle de fluxo regras invocadas. Os resultados do evento podem incluir indicadores de sucesso ou falha do evento e resultados específicos do evento (por exemplo, o estado de segurança do sistema de informações após a ocorrência do evento).  
  
**Melhorias do Controle:**

### AU-3(1): Conteúdo dos Registros de Auditoria | Informações Adicionais de Auditoria

O sistema de informações gera registros de auditoria contendo as seguintes informações adicionais: [Atribuição: informações adicionais e mais detalhadas definidas pela organização].  
Guia Adicional: As informações detalhadas que as organizações podem considerar nos registros de auditoria incluem, por exemplo, a gravação de texto completo de comandos privilegiados ou as identidades individuais dos usuários da conta do grupo. As organizações consideram limitar as informações de auditoria adicionais apenas às informações explicitamente necessárias para requisitos específicos de auditoria. Isso facilita o uso de trilhas de auditoria e logs de auditoria, não incluindo informações que possam ser enganosas ou que dificultem a localização de informações de interesse.

### AU-3(2): Conteúdo dos Registros de Auditoria | Gestão Centralizada Do Conteúdo Planejado Do Registro De Auditoria

O sistema de informações fornece gerenciamento e configuração centralizados do conteúdo a ser capturado nos registros de auditoria gerados por [Atribuição: componentes do sistema de informações definidos pela organização].  
Guia Adicional: Esse aprimoramento de controle exige que o conteúdo a ser capturado nos registros de auditoria seja configurado a partir de um local central (necessitando de automação). As organizações coordenam a seleção do conteúdo de auditoria necessário para dar suporte ao gerenciamento centralizado e ao recurso de configuração fornecido pelo sistema de informações.

## AU-4: Capacidade do Armazenamento de Auditoria (P1)

**Descrição do Controle:**A organização aloca a capacidade de armazenamento de registros de auditoria de acordo com [Atribuição: requisitos de armazenamento de registros de auditoria definidos pela organização].  
  
**Guia Adicional:**As organizações consideram os tipos de auditoria a serem executados e os requisitos de processamento de auditoria ao alocar a capacidade de armazenamento de auditoria. A alocação de capacidade de armazenamento de auditoria suficiente reduz a probabilidade de que essa capacidade seja excedida e resulta na possível perda ou redução da capacidade de auditoria.  
  
**Melhorias do Controle:**

### AU-4(1): Capacidade do Armazenamento de Auditoria | Transferir para Armazenamento Alternativo

O sistema de informações descarrega os registros de auditoria [Atribuição: frequência definida pela organização] em um sistema ou mídia diferente do sistema que está sendo auditado.  
Guia Adicional: O descarregamento é um processo projetado para preservar a confidencialidade e a integridade dos registros de auditoria, movendo os registros do sistema de informações primárias para um sistema secundário ou alternativo. É um processo comum em sistemas de informação com capacidade limitada de armazenamento de auditoria; o armazenamento de auditoria é usado apenas de maneira transitória até que o sistema possa se comunicar com o sistema secundário ou alternativo designado para armazenar os registros de auditoria, momento em que as informações são transferidas.

## AU-5: Resposta a Falhas de Processamento de Auditoria (P1)

**Descrição do Controle:**O sistema de informação:  
  
a. Alertas [Atribuição: pessoal ou funções definidos pela organização] no caso de uma falha no processamento da auditoria; e  
  
b. Realiza as seguintes ações adicionais: [Atribuição: ações definidas pela organização a serem tomadas (por exemplo, desligar o sistema de informações, substituir registros de auditoria mais antigos, interromper a geração de registros de auditoria)].  
  
**Guia Adicional:**As falhas no processamento de auditoria incluem, por exemplo, erros de software / hardware, falhas nos mecanismos de captura de auditoria e capacidade de armazenamento de auditoria alcançada ou excedida. As organizações podem optar por definir ações adicionais para diferentes falhas no processamento de auditoria (por exemplo, por tipo, por local, por gravidade ou por uma combinação desses fatores). Esse controle se aplica a cada repositório de armazenamento de dados de auditoria (ou seja, componente distinto do sistema de informações em que os registros de auditoria são armazenados), a capacidade total de armazenamento de auditoria das organizações (ou seja, todos os repositórios de armazenamento de dados de auditoria combinados) ou ambos.  
  
**Melhorias do Controle:**

### AU-5(1): Resposta a Falhas de Processamento de Auditoria | Capacidade de Armazenamento de Auditoria

O sistema de informações fornece um aviso para [Atribuição: pessoal, funções e/ou locais definidos pela organização] dentro de [Atribuição: período definido pela organização] quando o volume de armazenamento de registros de auditoria alocado atingir [Atribuição: porcentagem definida pela organização] do máximo do repositório capacidade de armazenamento de registros de auditoria.  
Guia Adicional: As organizações podem ter vários repositórios de armazenamento de dados de auditoria distribuídos por vários componentes do sistema de informações, com cada repositório tendo diferentes capacidades de volume de armazenamento.

### AU-5(2): Resposta a Falhas de Processamento de Auditoria | Alertas em Tempo Real

O sistema de informações fornece um alerta em [Atribuição: período em tempo real definido pela organização] para [Atribuição: pessoal, funções e/ou locais definidos pela organização] quando ocorrem os seguintes eventos de falha de auditoria: [Atribuição: falha de auditoria definida pela organização eventos que exigem alertas em tempo real].  
Guia Adicional: Os alertas fornecem às organizações mensagens urgentes. Alertas em tempo real fornecem essas mensagens na velocidade da tecnologia da informação (ou seja, o tempo entre a detecção do evento e o alerta ocorre em segundos ou menos).

### AU-5(3): Resposta a Falhas de Processamento de Auditoria | Limites de Volume de Tráfego Configuráveis

O sistema de informações impõe limites configuráveis de volume de tráfego de comunicações em rede, refletindo limites na capacidade de auditoria e [Seleção: rejeita; atrasos] tráfego de rede acima desses limites.  
Guia Adicional: As organizações têm a capacidade de rejeitar ou atrasar o processamento do tráfego de comunicações da rede se a auditoria desse tráfego for determinada para exceder a capacidade de armazenamento da função de auditoria do sistema de informação. A resposta de rejeição ou atraso é acionada pelos limites de volume de tráfego organizacional estabelecidos que podem ser ajustados com base nas alterações na capacidade de armazenamento de auditoria.

### AU-5(4): Resposta a Falhas de Processamento de Auditoria | Desligamento por Falha

O sistema de informações chama uma [Seleção: desligamento total do sistema; desligamento parcial do sistema; modo operacional degradado com funcionalidade limitada de missão / negócios disponível] no caso de [Atribuição: falhas de auditoria definidas pela organização], a menos que exista um recurso de auditoria alternativo.  
Guia Adicional: As organizações determinam os tipos de falhas de auditoria que podem acionar desligamentos automáticos do sistema de informações ou operações degradadas. Devido à importância de garantir a continuidade da missão / negócios, as organizações podem determinar que a natureza da falha na auditoria não seja tão grave que justifique o desligamento completo do sistema de informações que suporta as principais missões / operações organizacionais da empresa. Nesses casos, os desligamentos parciais do sistema de informações ou a operação em um modo degradado com capacidade reduzida podem ser alternativas viáveis.

## AU-6: Revisão, Análise e Relatório de Auditoria (P1)

**Descrição do Controle:**A organização:  
  
a. Analisa e analisa os registros de auditoria do sistema de informações [Tarefa: frequência definida pela organização] para obter indicações de [Tarefa: atividade inadequada ou incomum definida pela organização]; e  
  
b. Relata os resultados para [Atribuição: pessoal ou funções definidos pela organização].  
  
**Guia Adicional:**Auditoria revisão, análise e relatórios abrange auditoria de segurança de informações realizada por organizações, incluindo, por exemplo, auditoria que resulta de monitoramento de uso de conta, acesso remoto, conectividade sem fio, conexão de dispositivo móvel, configurações, inventário de componentes do sistema, uso de manutenção ferramentas e manutenção não-local, acesso físico, temperatura e umidade, entrega e remoção de equipamentos, comunicações nos limites do sistema de informação, uso de código móvel e uso de VoIP. Os resultados podem ser informados para entidades organizacionais que incluem, por exemplo, equipe de resposta a incidentes, help desk, grupo / departamento de segurança da informação. Se as organizações forem proibidas de revisar e analisar informações de auditoria ou não puderem realizar tais atividades (por exemplo, em determinados aplicativos ou sistemas de segurança nacional), a revisão / análise poderá ser realizada por outras organizações que tenham recebido tal autoridade.  
  
**Melhorias do Controle:**

### AU-6(1): Revisão, Análise e Relatório de Auditoria | Revisão da Auditoria, Análise e Integração de Processos

A organização emprega mecanismos automatizados para integrar os processos de revisão, análise e relatório de auditoria para apoiar os processos organizacionais de investigação e resposta a atividades suspeitas.  
Guia Adicional: Os processos organizacionais que se beneficiam da revisão, análise e relatório de auditoria integrados incluem, por exemplo, resposta a incidentes, monitoramento contínuo, planejamento de contingências e auditorias do Inspetor-Geral.

### AU-6(2): Revisão, Análise e Relatório de Auditoria | Revisão da Auditoria, Análise e Alertas De Segurança Automatizados

[Retirado: Incorporado no SI-4].

### AU-6(3): Revisão, Análise e Relatório de Auditoria | Revisão da Auditoria, Análise e Repositórios De Auditoria Correlatos

A organização analisa e correlaciona os registros de auditoria em diferentes repositórios para obter conhecimento da situação em toda a organização.  
Guia Adicional: A conscientização situacional em toda a organização inclui a conscientização nos três níveis de gerenciamento de riscos (ou seja, organizacional, missão / processos de negócios e sistema de informação) e apoia a conscientização entre organizações.

### AU-6(4): Revisão, Análise e Relatório de Auditoria | Revisão da Auditoria, Análise e Central de Revisão e Análise

O sistema de informações fornece a capacidade de revisar e analisar centralmente os registros de auditoria de vários componentes dentro do sistema.  
Guia Adicional: Mecanismos automatizados para revisões e análises centralizadas incluem, por exemplo, produtos de Gerenciamento de Informações de Segurança.

### AU-6(5): Revisão, Análise e Relatório de Auditoria | Revisão da Auditoria, Análise e Capacidade De Integração / Digitalização E Monitoramento

A organização integra a análise dos registros de auditoria com a análise de [Seleção (uma ou mais): informações sobre a verificação de vulnerabilidades; dados de desempenho; informações de monitoramento de sistemas de informação; [Atribuição: dados / informações definidos pela organização coletados de outras fontes]] para aprimorar ainda mais a capacidade de identificar atividades inadequadas ou incomuns.  
Guia Adicional: Esse aprimoramento de controle não requer varredura de vulnerabilidade, geração de dados de desempenho ou monitoramento do sistema de informações. Em vez disso, o aprimoramento exige que a análise das informações produzidas de outra forma nessas áreas seja integrada à análise das informações de auditoria. As ferramentas do Sistema de gerenciamento de informações e eventos de segurança podem facilitar a agregação / consolidação de registros de auditoria de vários componentes do sistema de informações, bem como a correlação e análise de registros de auditoria. O uso de scripts padronizados de análise de registros de auditoria desenvolvidos por organizações (com ajustes de scripts localizados, conforme necessário) fornece abordagens mais econômicas para analisar as informações coletadas dos registros de auditoria. A correlação das informações do registro de auditoria com as informações da varredura de vulnerabilidade é importante para determinar a veracidade das varreduras de vulnerabilidade e correlacionar os eventos de detecção de ataques aos resultados da varredura. A correlação com os dados de desempenho pode ajudar a descobrir ataques de negação de serviço ou ataques cibernéticos, resultando no uso não autorizado de recursos. A correlação com as informações de monitoramento do sistema pode ajudar a descobrir ataques e relacionar melhor as informações de auditoria às situações operacionais.

### AU-6(6): Revisão, Análise e Relatório de Auditoria | Revisão da Auditoria, Análise e Correlação com Monitoramento Físico

A organização correlaciona as informações dos registros de auditoria com as informações obtidas no monitoramento do acesso físico para aprimorar ainda mais a capacidade de identificar atividades suspeitas, inadequadas, incomuns ou malévolas.  
Guia Adicional: A correlação de informações de auditoria física e logs de auditoria de sistemas de informação pode ajudar as organizações a identificar exemplos de comportamento suspeito ou apoiar evidências desse comportamento. Por exemplo, a correlação da identidade de um indivíduo para acesso lógico a determinados sistemas de informações com as informações adicionais de segurança física que o indivíduo estava realmente presente na instalação quando o acesso lógico ocorreu, pode revelar-se útil nas investigações.

### AU-6(7): Revisão, Análise e Relatório de Auditoria | Revisão da Auditoria, Análise e Ações Permitidas

A organização especifica as ações permitidas para cada [Seleção (uma ou mais): processos do sistema de informação; Função; usuário] associado à revisão, análise e relatório de informações de auditoria.  
Guia Adicional: As organizações especificam ações permitidas para processos, funções e/ou usuários do sistema de informação associados à revisão, análise e relatório de registros de auditoria por meio de técnicas de gerenciamento de contas. A especificação de ações permitidas nas informações de auditoria é uma maneira de aplicar o princípio do menor privilégio. As ações permitidas são aplicadas pelo sistema de informações e incluem, por exemplo, ler, gravar, executar, anexar e excluir.

### AU-6(8): Revisão, Análise e Relatório de Auditoria | Revisão da Auditoria, Análise e Análise Completa de Textos de Comandos Privilegiados

A organização realiza uma análise de texto completo dos comandos privilegiados auditados em um componente ou subsistema fisicamente distinto do sistema de informações ou outro sistema de informações dedicado a essa análise.  
Guia Adicional: Esse aprimoramento de controle requer um ambiente distinto para a análise dedicada de informações de auditoria relacionadas a usuários privilegiados, sem comprometer essas informações no sistema de informações em que os usuários têm privilégios elevados, incluindo a capacidade de executar comandos privilegiados. A análise de texto completo refere-se à análise que considera o texto completo dos comandos privilegiados (isto é, comandos e todos os parâmetros), em oposição à análise que considera apenas o nome do comando. A análise de texto completo inclui, por exemplo, o uso de correspondência de padrões e heurísticas.

### AU-6(9): Revisão, Análise e Relatório de Auditoria | Revisão da Auditoria, Análise e Correlação Com Informação De Fontes Não Técnicas

A organização correlaciona informações de fontes não técnicas com informações de auditoria para aprimorar a conscientização situacional em toda a organização.  
Guia Adicional: As fontes não técnicas incluem, por exemplo, registros de recursos humanos que documentam violações das políticas organizacionais (por exemplo, incidentes de assédio sexual, uso inadequado de ativos de informações organizacionais). Essas informações podem levar as organizações a um esforço analítico mais direcionado para detectar possíveis atividades internas maliciosas. Devido à natureza sensível das informações disponíveis em fontes não técnicas, as organizações limitam o acesso a essas informações para minimizar o potencial de liberação inadvertida de informações relacionadas à privacidade a indivíduos que não precisam saber. Portanto, a correlação de informações de fontes não técnicas com informações de auditoria geralmente ocorre apenas quando há suspeita de indivíduos envolvidos em um incidente de segurança. As organizações obtêm aconselhamento jurídico antes de iniciar tais ações.

### AU-6(10): Revisão, Análise e Relatório de Auditoria | Revisão da Auditoria, Análise e Ajuste Do Nível De Auditoria

A organização ajusta o nível de revisão, análise e relatório de auditoria no sistema de informações quando há uma mudança no risco com base em informações policiais, informações de inteligência ou outras fontes credíveis de informações.  
Guia Adicional: A frequência, escopo e/ou profundidade da revisão, análise e relatório de auditoria podem ser ajustados para atender às necessidades organizacionais com base nas novas informações recebidas.

## AU-7: Resumo da Auditoria e Geração de Relatório (P2)

**Descrição do Controle:**O sistema de informações fornece um recurso de redução de auditoria e geração de relatórios que:  
  
a. Oferece suporte a requisitos de revisão, análise e relatório de auditoria sob demanda e investigações posteriores de incidentes de segurança; e  
  
b. Não altera o conteúdo original ou o pedido de tempo dos registros de auditoria.  
  
**Guia Adicional:**A redução de auditoria é um processo que manipula as informações de auditoria coletadas e as organiza em um formato de resumo que é mais significativo para os analistas. Os recursos de redução de auditoria e geração de relatórios nem sempre emanam do mesmo sistema de informações ou das mesmas entidades organizacionais que realizam atividades de auditoria. O recurso de redução de auditoria pode incluir, por exemplo, técnicas modernas de mineração de dados com filtros de dados avançados para identificar comportamentos anômalos nos registros de auditoria. A capacidade de geração de relatórios fornecida pelo sistema de informações pode gerar relatórios personalizáveis. A ordenação por horário dos registros de auditoria pode ser um problema significativo se a granularidade do registro de data e hora no registro for insuficiente.  
  
**Melhorias do Controle:**

### AU-7(1): Resumo da Auditoria e Geração de Relatório | Processamento Automático

O sistema de informações fornece a capacidade de processar registros de auditoria para eventos de interesse com base em [Atribuição: campos de auditoria definidos pela organização nos registros de auditoria].  
Guia Adicional: Eventos de interesse podem ser identificados pelo conteúdo de campos específicos de registros de auditoria, incluindo, por exemplo, identidades de indivíduos, tipos de eventos, locais de eventos, horários de eventos, datas de eventos, recursos de sistema envolvidos, endereços IP envolvidos ou objetos de informação acessados. As organizações podem definir critérios de eventos de auditoria com qualquer grau de granularidade necessário, por exemplo, locais selecionáveis por local geral de rede (por exemplo, por rede ou sub-rede) ou selecionável por componente específico do sistema de informações.

### AU-7(2): Resumo da Auditoria e Geração de Relatório | Classificação Automática e Pesquisa

O sistema de informações fornece a capacidade de classificar e pesquisar registros de auditoria por eventos de interesse com base no conteúdo de [Tarefa: campos de auditoria definidos pela organização nos registros de auditoria].  
Guia Adicional: A classificação e a pesquisa dos registros de auditoria podem ser baseadas no conteúdo dos campos dos registros de auditoria, por exemplo: (i) data / hora dos eventos; (ii) identificadores de usuários; (iii) endereços IP (Internet Protocol) envolvidos no evento; (iv) tipo de evento; ou (v) sucesso / falha do evento.

## AU-8: Marcação de Tempo (P1)

**Descrição do Controle:**O sistema de informação:  
  
a. Usa relógios internos do sistema para gerar registros de data e hora para registros de auditoria; e  
  
b. Registra registros de data e hora para registros de auditoria que podem ser mapeados para o Tempo Universal Coordenado (UTC) ou Horário de Greenwich (GMT) e atende a [Atribuição: granularidade de medida de tempo definida pela organização].  
  
**Guia Adicional:**Os timestamps gerados pelo sistema de informação incluem data e hora. A hora é normalmente expressa no Tempo Universal Coordenado (UTC), uma continuação moderna do Horário Médio de Greenwich (GMT) ou hora local com um deslocamento do UTC. A granularidade das medições de tempo refere-se ao grau de sincronização entre os relógios do sistema de informações e os relógios de referência, por exemplo, sincronizando os relógios em centenas de milissegundos ou em dezenas de milissegundos. As organizações podem definir diferentes granularidades de tempo para diferentes componentes do sistema. O serviço de horário também pode ser crítico para outros recursos de segurança, como controle de acesso, identificação e autenticação, dependendo da natureza dos mecanismos usados para dar suporte a esses recursos.  
  
**Melhorias do Controle:**

### AU-8(1): Marcação de Tempo | Sincronização com Fonte de Tempo Autoritária

O sistema de informação:  
  
a. Compara os relógios do sistema de informações internas [Atribuição: frequência definida pela organização] com [Atribuição: fonte de tempo autorizada definida pela organização]; e  
  
b. Sincroniza os relógios internos do sistema com a fonte de tempo autoritária quando a diferença de tempo é maior que [Atribuição: período definido pela organização].  
Guia Adicional: Esse aprimoramento de controle fornece uniformidade de carimbos de data / hora para sistemas de informações com vários relógios e sistemas conectados em uma rede.

### AU-8(2): Marcação de Tempo | Fonte Secundária de Tempo Autoritária

O sistema de informações identifica uma fonte de tempo com autoridade secundária localizada em uma região geográfica diferente da fonte de tempo com autoridade primária.

## AU-9: Proteção das Informações de Auditoria (P1)

**Descrição do Controle:**O sistema de informações protege as informações de auditoria e as ferramentas de auditoria contra acesso não autorizado, modificação e exclusão.  
  
**Guia Adicional:**As informações de auditoria incluem todas as informações necessárias (por exemplo, registros de auditoria, configurações de auditoria e relatórios de auditoria) para auditar com êxito a atividade do sistema de informações. Esse controle se concentra na proteção técnica das informações de auditoria. A proteção física das informações de auditoria é tratada por controles de proteção de mídia e controles de proteção física e ambiental.  
  
**Melhorias do Controle:**

### AU-9(1): Proteção das Informações de Auditoria | Meios de Gravação de Hardware

O sistema de informações grava trilhas de auditoria em mídia de gravação única aplicada por hardware.  
Guia Adicional: Esse aprimoramento de controle se aplica à geração inicial de trilhas de auditoria (ou seja, à coleta de registros de auditoria que representam as informações de auditoria a serem usadas para fins de detecção, análise e relatório) e ao backup dessas trilhas de auditoria. O aprimoramento não se aplica à geração inicial de registros de auditoria antes de ser gravada em uma trilha de auditoria. A mídia WORM (gravação única) e leitura múltipla inclui, por exemplo, CD-R (Compact Disk Recordable) e DVD-R (Digital Video Disk Recordable). Por outro lado, o uso de mídia comutável de proteção contra gravação, como em cartuchos de fita ou unidades USB (Universal Serial Bus), resulta em mídia protegida contra gravação, mas não com gravação única.

### AU-9(2): Proteção das Informações de Auditoria | Backup de Auditoria em Sistemas / Componentes Físicos Separados

O sistema de informações faz backup dos registros de auditoria [Atribuição: frequência definida pela organização] em um sistema ou componentes de sistema fisicamente diferente do sistema ou componente que está sendo auditado.  
Guia Adicional: Esse aprimoramento de controle ajuda a garantir que um comprometimento do sistema de informações que está sendo auditado também não resulte em comprometimento dos registros de auditoria.

### AU-9(3): Proteção das Informações de Auditoria | Proteção Criptográfica

O sistema de informações implementa mecanismos criptográficos para proteger a integridade das informações e ferramentas de auditoria.  
Guia Adicional: Os mecanismos criptográficos usados para proteger a integridade das informações de auditoria incluem, por exemplo, funções de hash assinadas usando criptografia assimétrica, permitindo a distribuição da chave pública para verificar as informações de hash, mantendo a confidencialidade da chave secreta usada para gerar o hash.

### AU-9(4): Proteção das Informações de Auditoria | Acesso por Subgrupo de Usuários Privilegiados

A organização autoriza o acesso ao gerenciamento da funcionalidade de auditoria apenas para [Atribuição: subconjunto de usuários privilegiados definido pela organização].  
Guia Adicional: Indivíduos com acesso privilegiado a um sistema de informações e que também são objeto de uma auditoria por esse sistema, podem afetar a confiabilidade das informações de auditoria inibindo as atividades de auditoria ou modificando os registros de auditoria. Esse aprimoramento de controle exige que o acesso privilegiado seja definido mais entre privilégios relacionados à auditoria e outros privilégios, limitando assim os usuários com privilégios relacionados à auditoria.

### AU-9(5): Proteção das Informações de Auditoria | Autorização Dupla

A organização impõe autorização dupla para [Seleção (um ou mais): movimento; exclusão] de [Cessão: informações de auditoria definidas pela organização].  
Guia Adicional: As organizações podem escolher opções de seleção diferentes para diferentes tipos de informações de auditoria. Mecanismos duplos de autorização exigem a aprovação de dois indivíduos autorizados para execução. A autorização dupla também pode ser conhecida como controle de duas pessoas.

### AU-9(6): Proteção das Informações de Auditoria | Acesso de Somente Leitura

A organização autoriza o acesso somente leitura às informações de auditoria para [Atribuição: subconjunto definido pela organização de usuários privilegiados].  
Guia Adicional: A restrição de autorizações de usuário privilegiadas para somente leitura ajuda a limitar os possíveis danos às organizações que podem ser iniciados por esses usuários (por exemplo, excluir registros de auditoria para encobrir atividades maliciosas).

## AU-10: Não-Repúdio (P2)

**Descrição do Controle:**O sistema de informação protege contra um indivíduo (ou processo agindo em nome de um indivíduo) negando falsamente ter realizado [Atribuição: ações definidas pela organização para serem cobertas pelo não-repúdio].  
  
**Guia Adicional:**Tipos de ações individuais cobertas por não-repúdio incluem, por exemplo, criar informações, enviar e receber mensagens, aprovar informações (por exemplo, indicando concordância ou assinar um contrato). O não-repúdio protege os indivíduos contra reclamações posteriores por: (i) autores de não terem escrito determinados documentos; (ii) remetentes por não terem transmitido mensagens; (iii) destinatários por não terem recebido mensagens; ou (iv) signatários de não ter documentos assinados. Os serviços de não repúdio podem ser usados para determinar se as informações foram originadas de um indivíduo em particular ou se um indivíduo realizou ações específicas (por exemplo, enviando um e-mail, assinando um contrato, aprovando uma solicitação de aquisição) ou recebendo informações específicas. As organizações obtêm serviços de não repúdio empregando várias técnicas ou mecanismos (por exemplo, assinaturas digitais, recibos de mensagens digitais).  
  
**Melhorias do Controle:**

### AU-10(1): Não-Repúdio | Associação de Identidades

O sistema de informação:  
  
a. Vincula a identidade do produtor de informações com as informações a [Atribuição: força de ligação definida pela organização]; e  
  
b. Fornece os meios para indivíduos autorizados determinarem a identidade do produtor da informação.  
Guia Adicional: Esse aprimoramento de controle suporta os requisitos de auditoria que fornecem ao pessoal organizacional os meios para identificar quem produziu informações específicas no caso de uma transferência de informações. As organizações determinam e aprovam a força da ligação entre o produtor e as informações, com base na categoria de segurança das informações e nos fatores de risco relevantes.

### AU-10(2): Não-Repúdio | Ligação Não-Validada da Informação sobre a Identidade do Produtor

O sistema de informação:  
  
a. Valida a ligação da identidade do produtor de informações às informações em [Atribuição: frequência definida pela organização]; e  
  
b. Executa [Atribuição: ações definidas pela organização] no caso de um erro de validação.  
Guia Adicional: Esse aprimoramento de controle impede a modificação de informações entre produção e revisão. A validação de ligações pode ser alcançada, por exemplo, pelo uso de somas de verificação criptográficas. As organizações determinam se as validações são em resposta a solicitações do usuário ou geradas automaticamente.

### AU-10(3): Não-Repúdio | Cadeia de Custodia

O sistema de informações mantém a identidade e as credenciais do revisor / liberador dentro da cadeia de custódia estabelecida para todas as informações revisadas ou liberadas.  
Guia Adicional: A cadeia de custódia é um processo que rastreia o movimento da evidência através de seu ciclo de vida de coleta, proteção e análise, documentando cada pessoa que lidou com a evidência, a data e a hora em que ela foi coletada ou transferida e o objetivo da transferência. Se o revisor é humano ou se a função de revisão é automatizada, mas separada da função de liberação / transferência, o sistema de informações associa a identidade do revisor das informações a serem liberadas com as informações e o rótulo das informações. No caso de análises humanas, esse aprimoramento de controle fornece aos funcionários da organização os meios para identificar quem revisou e divulgou as informações. No caso de revisões automatizadas, esse aprimoramento de controle garante que apenas as funções de revisão aprovadas sejam empregadas.

### AU-10(4): Não-Repúdio | Validação da Identidade do Revisor de Informação

O sistema de informação:  
  
a. Valida a ligação da identidade do revisor de informações às informações nos pontos de transferência ou liberação antes da liberação / transferência entre [Atribuição: domínios de segurança definidos pela organização]; e  
  
b. Executa [Atribuição: ações definidas pela organização] no caso de um erro de validação.  
Guia Adicional: Esse aprimoramento de controle impede a modificação de informações entre revisão e transferência / liberação. A validação de ligações pode ser alcançada, por exemplo, pelo uso de somas de verificação criptográficas. As organizações determinam que as validações são em resposta a solicitações do usuário ou geradas automaticamente.

### AU-10(5): Não-Repúdio | Assinaturas Digitais

[Retirado: Incorporado no SI-7].

## AU-11: Retenção dos Dados de Auditoria (P3)

**Descrição do Controle:**A organização mantém registros de auditoria por [Atribuição: período definido pela organização de acordo com a política de retenção de registros] para fornecer suporte para investigações posteriores de incidentes de segurança e para atender aos requisitos regulatórios e de retenção de informações organizacionais.  
  
**Guia Adicional:**As organizações retêm registros de auditoria até que seja determinado que não são mais necessários para fins administrativos, legais, de auditoria ou outros fins operacionais. Isso inclui, por exemplo, retenção e disponibilidade de registros de auditoria relativos a solicitações, intimações e ações de aplicação da lei da Lei de Liberdade de Informação (FOIA). As organizações desenvolvem categorias padrão de registros de auditoria relativos a esses tipos de ações e processos de resposta padrão para cada tipo de ação. As agendas de registros gerais da Administração Nacional de Arquivos e Registros (NARA) fornecem uma política federal de retenção de registros.  
  
**Melhorias do Controle:**

### AU-11(1): Retenção dos Dados de Auditoria | Capacidade de Recuperação a Longo Prazo

A organização emprega [Atribuição: medidas definidas pela organização] para garantir que os registros de auditoria de longo prazo gerados pelo sistema de informações possam ser recuperados.  
Guia Adicional: As medidas empregadas pelas organizações para ajudar a facilitar a recuperação dos registros de auditoria incluem, por exemplo, a conversão de registros em formatos mais recentes, a retenção de equipamentos capazes de ler os registros e a documentação necessária para ajudar o pessoal organizacional a entender como interpretar os registros.

## AU-12: Geração de Auditoria (P1)

**Descrição do Controle:**O sistema de informação:  
  
a. Fornece capacidade de geração de registros de auditoria para os eventos auditáveis definidos em AU-2 a. em [Atribuição: componentes do sistema de informações definidos pela organização];  
  
b. Permite que [Atribuição: pessoal ou funções definidas pela organização] selecione quais eventos auditáveis devem ser auditados por componentes específicos do sistema de informação; e  
  
c. Gera registros de auditoria para os eventos definidos em AU-2(d) com o conteúdo definido em AU-3.  
  
**Guia Adicional:**Registros de auditoria podem ser gerados a partir de diversos componentes do sistema de informações. A lista de eventos auditados é o conjunto de eventos para os quais as auditorias devem ser geradas. Esses eventos geralmente são um subconjunto de todos os eventos para os quais o sistema de informações é capaz de gerar registros de auditoria.  
  
**Melhorias do Controle:**

### AU-12(1): Geração de Auditoria | Trilha de Auditoria Larga do Sistema / Correlata por Tempo

O sistema de informações compila registros de auditoria de [Atribuição: componentes do sistema de informações definidos pela organização] em uma trilha de auditoria (lógica ou física) em todo o sistema, que é correlacionada no tempo com [Atribuição: nível de tolerância definido pela organização para a relação entre o tempo selos de registros individuais na trilha de auditoria].  
Guia Adicional: As trilhas de auditoria são correlacionadas com o tempo se os registros de data e hora nos registros de auditoria individuais puderem ser relacionados de maneira confiável aos registros de data e hora em outros registros de auditoria para obter uma ordem de tempo dos registros dentro das tolerâncias organizacionais.

### AU-12(2): Geração de Auditoria | Formatos Padronizados

O sistema de informações produz uma trilha de auditoria em todo o sistema (lógica ou física) composta por registros de auditoria em um formato padronizado.  
Guia Adicional: As informações de auditoria normalizadas para padrões comuns promovem a interoperabilidade e o intercâmbio dessas informações entre dispositivos e sistemas de informação diferentes. Isso facilita a produção de informações de eventos que podem ser mais prontamente analisadas e correlacionadas. Os formatos padrão para registros de auditoria incluem, por exemplo, registros de log do sistema e registros de auditoria compatíveis com CEE (Common Event Expressions). Se os mecanismos de registro nos sistemas de informações não estiverem em conformidade com os formatos padronizados, os sistemas poderão converter registros de auditoria individuais em formatos padronizados ao compilar trilhas de auditoria em todo o sistema.

### AU-12(3): Geração de Auditoria | Alterações por Indivíduos Autorizados

O sistema de informações fornece a capacidade para [Atribuição: indivíduos ou funções definidos pela organização] alterar a auditoria a ser executada em [Atribuição: componentes do sistema de informações definidos pela organização] com base em [Atribuição: critérios de eventos selecionáveis definidos pela organização] em [Atribuição : limites de tempo definidos pela organização].  
Guia Adicional: Esse aprimoramento de controle permite que as organizações estendam ou limitem a auditoria conforme necessário para atender aos requisitos organizacionais. A auditoria limitada para conservar os recursos do sistema de informações pode ser estendida para lidar com determinadas situações de ameaça. Além disso, a auditoria pode ser limitada a um conjunto específico de eventos para facilitar a redução, análise e geração de relatórios. As organizações podem estabelecer limites de tempo nos quais as ações de auditoria são alteradas, por exemplo, quase em tempo real, em minutos ou em horas.

## AU-13: Monitoramento da Divulgação de Informações (P0)

**Descrição do Controle:**A organização monitora [Atribuição: informações de fonte aberta e/ou sites de informações definidas pela organização] [Atribuição: frequência definida pela organização] para evidência de divulgação não autorizada de informações organizacionais.  
  
**Guia Adicional:**As informações de código aberto incluem, por exemplo, sites de redes sociais.  
  
**Melhorias do Controle:**

### AU-13(1): Monitoramento da Divulgação de Informações | Uso de Ferramentas Automatizadas

A organização emprega mecanismos automatizados para determinar se as informações organizacionais foram divulgadas de maneira não autorizada.  
Guia Adicional: Os mecanismos automatizados podem incluir, por exemplo, scripts automatizados para monitorar novas postagens em sites selecionados e serviços comerciais que fornecem notificações e alertas para as organizações.

### AU-13(2): Monitoramento da Divulgação de Informações | Revisão de Sites Monitorados

A organização revisa os sites de informações de código aberto que estão sendo monitorados [Atribuição: frequência definida pela organização].

## AU-14: Auditoria da Sessão (P0)

**Descrição do Controle:**O sistema de informações fornece a capacidade para usuários autorizados selecionarem uma sessão de usuário para capturar / gravar ou visualizar / ouvir.  
  
**Guia Adicional:**Auditorias de sessão incluem, por exemplo, monitoramento de teclas, rastreamento de sites visitados e registro de informações e/ou transferências de arquivos. As atividades de auditoria de sessão são desenvolvidas, integradas e usadas em consulta com a assessoria jurídica de acordo com as leis federais, ordens executivas, diretivas, políticas, regulamentos ou normas aplicáveis.  
  
**Melhorias do Controle:**

### AU-14(1): Auditoria da Sessão | Inicialização do Sistema

O sistema de informações inicia auditorias de sessão na inicialização do sistema.

### AU-14(2): Auditoria da Sessão | Captura/Gravação e Conteúdo de Log

O sistema de informações oferece aos usuários autorizados a capacidade de capturar / registrar e registrar o conteúdo relacionado a uma sessão do usuário.

### AU-14(3): Auditoria da Sessão | Visualização/Escuta Remota

O sistema de informações oferece aos usuários autorizados a capacidade de visualizar / ouvir remotamente todo o conteúdo relacionado a uma sessão estabelecida do usuário em tempo real.

## AU-15: Capacidade de Auditoria Alternativa (P0)

**Descrição do Controle:**A organização fornece um recurso de auditoria alternativo no caso de uma falha no recurso de auditoria principal que fornece [Atribuição: funcionalidade de auditoria alternativa definida pela organização].  
  
**Guia Adicional:**Como um recurso de auditoria alternativo pode ser uma proteção de curto prazo empregada até que a falha no recurso de auditoria principal seja corrigida, as organizações podem determinar que o recurso de auditoria alternativo precisa fornecer apenas um subconjunto da funcionalidade de auditoria primária afetada pela falha.

## AU-16: Auditoria Organizacional Transversal (P0)

**Descrição do Controle:**A organização emprega [Atribuição: métodos definidos pela organização] para coordenar [Atribuição: informações de auditoria definidas pela organização] entre organizações externas quando as informações de auditoria são transmitidas através dos limites organizacionais.  
  
**Guia Adicional:**Quando as organizações usam sistemas de informação e/ou serviços de organizações externas, o recurso de auditoria exige uma abordagem coordenada entre as organizações. Por exemplo, manter a identidade de indivíduos que solicitaram serviços específicos além dos limites organizacionais pode ser muitas vezes muito difícil, e isso pode resultar em ramificações significativas no desempenho. Portanto, geralmente é o caso da auditoria entre organizações (por exemplo, o tipo de recurso de auditoria fornecido pelas arquiteturas orientadas a serviços) simplesmente captura a identidade dos indivíduos que emitem solicitações no sistema de informações inicial e os sistemas subsequentes registram que as solicitações emanaram de indivíduos autorizados.  
  
**Melhorias do Controle:**

### AU-16(1): Auditoria Organizacional Transversal | Preservação de Identidade

A organização exige que a identidade dos indivíduos seja preservada nas trilhas de auditoria entre organizações.  
Guia Adicional: Esse aprimoramento de controle se aplica quando é necessário rastrear ações que são executadas através dos limites da organização para um indivíduo específico.

### AU-16(2): Auditoria Organizacional Transversal | Compartilhamento das Informações de Auditoria

A organização fornece informações de auditoria entre organizações para [Atribuição: organizações definidas pela organização] com base em [Atribuição: acordos de compartilhamento entre organizações definidas pela organização].  
Guia Adicional: Devido à natureza distribuída das informações de auditoria, o compartilhamento entre organizações das informações de auditoria pode ser essencial para uma análise eficaz da auditoria que está sendo realizada. Por exemplo, os registros de auditoria de uma organização podem não fornecer informações suficientes para determinar o uso apropriado ou inadequado de recursos de informações organizacionais por indivíduos em outras organizações. Em alguns casos, apenas as organizações de origem dos indivíduos têm o conhecimento apropriado para fazer essas determinações, exigindo, portanto, o compartilhamento de informações de auditoria entre as organizações.

# AT - Conscientização e Treinamento

## AT-1: Política e Procedimentos de Conscientização e Formação em Segurança (P1)

**Descrição do Controle:**A organização:  
  
a. Desenvolve, documenta e dissemina para [Atribuição: pessoal ou funções definidas pela organização]:  
  
1. Uma política de conscientização e treinamento de segurança que lide com propósito, escopo, funções, responsabilidades, compromisso de gerenciamento, coordenação entre entidades organizacionais e conformidade; e  
  
2. Procedimentos para facilitar a implementação da política de conscientização e treinamento sobre segurança e conscientização associada de segurança e controles de treinamento; e  
  
b. Revisa e atualiza a atual:  
  
1. Política de conscientização e treinamento de segurança [Atribuição: frequência definida pela organização]; e  
  
2. Conscientização sobre segurança e procedimentos de treinamento [Atribuição: frequência definida pela organização].  
  
**Guia Adicional:**Esse controle aborda o estabelecimento de políticas e procedimentos para a implementação efetiva de controles de segurança selecionados e aprimoramentos de controle na família AT. As políticas e procedimentos refletem as leis federais aplicáveis, ordens executivas, diretivas, regulamentos, políticas, normas e diretrizes. Políticas e procedimentos do programa de segurança no nível da organização podem tornar desnecessária a necessidade de políticas e procedimentos específicos do sistema. A política pode ser incluída como parte da política geral de segurança da informação para organizações ou, inversamente, pode ser representada por múltiplas políticas refletindo a natureza complexa de certas organizações. Os procedimentos podem ser estabelecidos para o programa de segurança em geral e para sistemas de informação específicos, se necessário. A estratégia de gerenciamento de risco organizacional é um fator chave no estabelecimento de políticas e procedimentos.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-12 | https://csrc.nist.gov/publications/search?keywords-lg=800-12 |
| Publicação Especial NIST 800-16 | https://csrc.nist.gov/publications/search?keywords-lg=800-16 |
| Publicação Especial NIST 800-50 | https://csrc.nist.gov/publications/search?keywords-lg=800-50 |
| Publicação Especial NIST 800-100 | https://csrc.nist.gov/publications/search?keywords-lg=800-100 |

## AT-2: Treinamento de Conscientização em Segurança (P1)

**Descrição do Controle:**A organização fornece treinamento básico de conscientização de segurança para usuários do sistema de informações (incluindo gerentes, executivos seniores e contratados):  
  
a. Como parte do treinamento inicial para novos usuários;  
  
b. Quando exigido pelas alterações do sistema de informação; e  
  
c. [Atribuição: frequência definida-organização] depois.  
  
**Guia Adicional:**As organizações determinam o conteúdo apropriado do treinamento de conscientização de segurança e técnicas de conscientização de segurança com base nos requisitos organizacionais específicos e nos sistemas de informações para os quais o pessoal autorizou o acesso. O conteúdo inclui uma compreensão básica da necessidade de segurança da informação e ações do usuário para manter a segurança e responder a incidentes de segurança suspeitos. O conteúdo também aborda a conscientização sobre a necessidade de segurança nas operações. As técnicas de conscientização de segurança podem incluir, por exemplo, a exibição de cartazes, fornecimento de suprimentos inscritos com lembretes de segurança, geração de avisos / avisos por e-mail de altos funcionários da organização, exibição de mensagens na tela de login e realização de eventos de conscientização de segurança da informação.  
  
**Melhorias do Controle:**

### AT-2(1): Treinamento de Conscientização em Segurança | Exercícios Práticos

A organização inclui exercícios práticos em treinamento de conscientização de segurança que simulam ataques cibernéticos reais.  
Guia Adicional: Os exercícios práticos podem incluir, por exemplo, tentativas de engenharia social sem aviso prévio para coletar informações, obter acesso não autorizado ou simular o impacto adverso de abrir anexos de e-mail maliciosos ou invocar, por meio de ataques de spear phishing, links maliciosos da web.

### AT-2(2): Treinamento de Conscientização em Segurança | Ameaça Interna

A organização inclui treinamento de conscientização sobre segurança no reconhecimento e relato de potenciais indicadores de ameaças internas.  
Guia Adicional: Indicadores potenciais e possíveis precursores de ameaças internas podem incluir comportamentos como insatisfação excessiva e prolongada no trabalho, tentativas de obter acesso a informações não necessárias para o desempenho no trabalho, acesso inexplicável a recursos financeiros, intimidação ou assédio sexual de colegas de trabalho, violência no local de trabalho, e outras violações graves de políticas, procedimentos, diretrizes, regras ou práticas organizacionais. O treinamento de conscientização de segurança inclui como comunicar as preocupações dos funcionários e da gerência com relação a indicadores potenciais de ameaças internas por meio de canais organizacionais apropriados, de acordo com as políticas e procedimentos organizacionais estabelecidos.

**Referências:**

|  |  |
| --- | --- |
| Código de Regulamentos Federais - 5 CFR 930.301 | https://www.govinfo.gov/app/details/CFR-2009-title5-vol2/CFR-2009-title5-vol2-sec930-301 |
| Ordem Executiva da Casa Branca Nº13587 | http://www.whitehouse.gov/the-press-office/2011/10/07/executive-order-13587-structural-reforms-improve-security-classified-net |
| Publicação Especial NIST 800-50 | https://csrc.nist.gov/publications/search?keywords-lg=800-50 |

## AT-3: Treinamento de Segurança Baseado em Cargo (P1)

**Descrição do Controle:**A organização fornece treinamento de segurança baseado no cargo dos funcionários com funções e responsabilidades de segurança atribuídas:  
  
a. Antes de autorizar o acesso ao sistema de informações ou executar tarefas atribuídas;  
  
b. Quando exigido pelas alterações do sistema de informação; e  
  
c. A cada [Atribuição: frequência definida-organização].  
  
**Guia Adicional:**As organizações determinam o conteúdo apropriado do treinamento de segurança com base nas funções e responsabilidades atribuídas dos indivíduos e nos requisitos de segurança específicos das organizações e nos sistemas de informações para os quais o pessoal autorizou o acesso. Além disso, as organizações fornecem arquitetos empresariais, desenvolvedores de sistemas de informação, desenvolvedores de software, funcionários de aquisições / aquisições, gerentes de sistemas de informação, administradores de sistema / rede, pessoal conduzindo atividades de gerenciamento e auditoria de configuração, pessoal executando atividades de verificação e validação independentes, assessores de controle de segurança e outro pessoal que tenha acesso ao software no nível do sistema, treinamento técnico adequado relacionado à segurança, especificamente adaptado às tarefas atribuídas. O treinamento abrangente baseado em funções aborda funções e responsabilidades técnicas, operacionais e de gerenciamento que abrangem proteções e contramedidas físicas, pessoais e técnicas. Esse treinamento pode incluir, por exemplo, políticas, procedimentos, ferramentas e artefatos para as funções de segurança organizacional definidas. As organizações também fornecem o treinamento necessário para que os indivíduos cumpram suas responsabilidades relacionadas às operações e à segurança da cadeia de suprimentos dentro do contexto dos programas de segurança da informação organizacionais. O treinamento em segurança baseado em funções também se aplica a prestadores de serviços que prestam serviços a agências federais.  
  
**Melhorias do Controle:**

### AT-3(1): Treinamento de Segurança Baseado em Cargo | Controles Ambientais

A organização fornece [Atribuição: pessoal ou funções definidas pela organização] treinamento inicial e [Atribuição: frequência definida pela organização] no emprego e operação de controles ambientais.  
Guia Adicional: Os controles ambientais incluem, por exemplo, dispositivos / sistemas de supressão e detecção de incêndio, sistemas de aspersão, extintores de mão, mangueiras fixas de incêndio, detectores de fumaça, temperatura / umidade, HVAC e energia dentro da instalação. As organizações identificam pessoal com funções e responsabilidades específicas associadas aos controles ambientais que exigem treinamento especializado.

### AT-3(2): Treinamento de Segurança Baseado em Cargo | Controles de Segurança Física

A organização fornece [Atribuição: pessoal ou funções definidas pela organização] treinamento inicial e [Atribuição: frequência definida pela organização] no emprego e operação de controles de segurança física.  
Guia Adicional: Os controles de segurança física incluem, por exemplo, dispositivos de controle de acesso físico, alarmes de intrusão física, equipamentos de monitoramento / vigilância e guardas de segurança (procedimentos de implantação e operação). As organizações identificam pessoal com funções e responsabilidades específicas associadas aos controles de segurança física que exigem treinamento especializado.

### AT-3(3): Treinamento de Segurança Baseado em Cargo | Exercícios Práticos

A organização inclui exercícios práticos em treinamento de segurança que reforçam os objetivos do treinamento.  
Guia Adicional: Os exercícios práticos podem incluir, por exemplo, treinamento de segurança para desenvolvedores de software que inclui ataques cibernéticos simulados que exploram vulnerabilidades comuns de software (por exemplo, estouros de buffer) ou ataques de phishing de lança / baleia direcionados a líderes / executivos seniores. Esses tipos de exercícios práticos ajudam os desenvolvedores a entender melhor os efeitos de tais vulnerabilidades e a apreciar a necessidade de padrões e processos de codificação de segurança.

### AT-3(4): Treinamento de Segurança Baseado em Cargo | Comunicações Suspensas e Comportamento Anormal de Sistemas

A organização fornece treinamento ao seu pessoal em [Atribuição: indicadores definidos pela organização de código malicioso] para reconhecer comunicações suspeitas e comportamento anômalo nos sistemas de informações organizacionais.  
Guia Adicional: Uma força de trabalho bem treinada fornece outra proteção organizacional que pode ser empregada como parte de uma estratégia de defesa profunda para proteger as organizações contra códigos maliciosos que chegam às organizações por e-mail ou aplicativos da Web. O pessoal é treinado para procurar indicações de e-mail potencialmente suspeito (por exemplo, receber um e-mail inesperado, receber um e-mail com gramática estranha ou ruim ou receber um e-mail de um remetente desconhecido, mas que parece ser de um patrocinador ou contratado conhecido). O pessoal também é treinado sobre como responder a e-mails suspeitos ou comunicações na Web (por exemplo, não abrir anexos, não clicar em links da Web incorporados e verificar a origem dos endereços de e-mail). Para que esse processo funcione efetivamente, todo o pessoal da organização é treinado e ciente do que constitui uma comunicação suspeita. O treinamento de pessoal sobre como reconhecer comportamentos anômalos em sistemas de informações organizacionais pode fornecer um alerta precoce para a presença de código malicioso. O reconhecimento desse comportamento anômalo pelo pessoal da organização pode complementar as ferramentas e sistemas automatizados de detecção e proteção de código malicioso empregados pelas organizações.

**Referências:**

|  |  |
| --- | --- |
| Código de Regulamentos Federais - 5 CFR 930.301 | https://www.govinfo.gov/app/details/CFR-2009-title5-vol2/CFR-2009-title5-vol2-sec930-301 |
| Publicação Especial NIST 800-16 | https://csrc.nist.gov/publications/search?keywords-lg=800-16 |
| Publicação Especial NIST 800-50 | https://csrc.nist.gov/publications/search?keywords-lg=800-50 |

## AT-4: Registros de Treinamento de Segurança (P3)

**Descrição do Controle:**A organização:  
  
a. Documenta e monitora as atividades de treinamento de segurança do sistema de informações individuais, incluindo treinamento básico de conscientização de segurança e treinamento específico de segurança do sistema de informações; e  
  
b. Mantém registros de treinamento individuais para [Atribuição: período de tempo definido pela organização].  
  
**Guia Adicional:**A documentação para treinamento especializado pode ser mantida por supervisores individuais, a critério da organização.

## AT-5: Contatos com Grupos de Segurança e Associações (P0)

**Descrição do Controle:**[Retirado: Incorporado na PM-15].

# CM - Gestão de Configurações

## CM-1: Política e Procedimentos de Gestão da Configuração (P1)

**Descrição do Controle:**A organização:  
  
a. Desenvolve, documenta e divulga para [Atribuição: pessoal ou funções definidas pela organização]:  
  
1. Uma política de gerenciamento de configuração que aborda finalidade, escopo, funções, responsabilidades, comprometimento do gerenciamento, coordenação entre entidades organizacionais e conformidade; e  
  
2. Procedimentos para facilitar a implementação da política de gerenciamento de configuração e controles de gerenciamento de configuração associados; e  
  
b. Revisa e atualiza o atual:  
  
1. Política de gerenciamento de configuração [Atribuição: frequência definida pela organização]; e  
  
2. Procedimentos de gerenciamento de configuração [Atribuição: frequência definida pela organização].  
  
**Guia Adicional:**Esse controle aborda o estabelecimento de políticas e procedimentos para a implementação efetiva de controles de segurança selecionados e aprimoramentos de controle na família CM. As políticas e procedimentos refletem as leis federais aplicáveis, ordens executivas, diretivas, regulamentos, políticas, normas e diretrizes. Políticas e procedimentos do programa de segurança no nível da organização podem tornar desnecessária a necessidade de políticas e procedimentos específicos do sistema. A política pode ser incluída como parte da política geral de segurança da informação para organizações ou, inversamente, pode ser representada por múltiplas políticas refletindo a natureza complexa de certas organizações. Os procedimentos podem ser estabelecidos para o programa de segurança em geral e para sistemas de informação específicos, se necessário. A estratégia de gerenciamento de risco organizacional é um fator chave no estabelecimento de políticas e procedimentos.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-12 | https://csrc.nist.gov/publications/search?keywords-lg=800-12 |
| Publicação Especial NIST 800-100 | https://csrc.nist.gov/publications/search?keywords-lg=800-100 |

## CM-2: Configuração Base de Referência (P1)

**Descrição do Controle:**A organização desenvolve, documenta e mantém sob controle de configuração, uma configuração atual da linha de base do sistema de informações.  
  
**Guia Adicional:**Esse controle estabelece configurações de linha de base para sistemas de informação e componentes do sistema, incluindo aspectos relacionados à comunicação e à conectividade dos sistemas. As configurações de linha de base são conjuntos de especificações documentados, revisados formalmente e acordados para sistemas de informação ou itens de configuração dentro desses sistemas. As configurações de linha de base servem como base para futuros builds, releases e/ou alterações nos sistemas de informação. Configurações de linha de base incluem informações sobre componentes do sistema de informações (por exemplo, pacotes de software padrão instalados em estações de trabalho, computadores notebook, servidores, componentes de rede ou dispositivos móveis; números de versão atuais e informações de patch em sistemas operacionais e aplicativos; configurações / parâmetros) topologia e o posicionamento lógico desses componentes na arquitetura do sistema. A manutenção de configurações de linha de base requer a criação de novas linhas de base à medida que os sistemas de informações organizacionais mudam com o tempo. As configurações de linha de base dos sistemas de informação refletem a arquitetura corporativa atual.  
  
**Melhorias do Controle:**

### CM-2(1): Configuração Base de Referência | Revisões e Atualizações

A organização revisa e atualiza a configuração da linha de base do sistema de informações:  
  
a. [Tarefa: frequência definida pela organização];  
  
b. Quando necessário devido a [circunstâncias definidas pela organização da atribuição]; e  
  
c. Como parte integrante das instalações e atualizações dos componentes do sistema de informação.

### CM-2(2): Configuração Base de Referência | Suporte de Automação para Precisão

A organização emprega mecanismos automatizados para manter uma configuração de linha de base atualizada, completa, precisa e prontamente disponível do sistema de informações.  
Guia Adicional: Mecanismos automatizados que ajudam as organizações a manter configurações consistentes de linha de base para sistemas de informação incluem, por exemplo, ferramentas de inventário de hardware e software, ferramentas de gerenciamento de configuração e ferramentas de gerenciamento de rede. Essas ferramentas podem ser implantadas e/ou alocadas como controles comuns, no nível do sistema de informações ou no nível do sistema operacional ou do componente (por exemplo, em estações de trabalho, servidores, notebooks, componentes de rede ou dispositivos móveis). As ferramentas podem ser usadas, por exemplo, para rastrear números de versão em aplicativos do sistema operacional, tipos de softwares instalados e níveis de patch atuais. Esse aprimoramento de controle pode ser satisfeito com a implementação do CM-8 (2) para organizações que optam por combinar o inventário de componentes do sistema de informações e as atividades de configuração da linha de base.

### CM-2(3): Configuração Base de Referência | Retenção de Configurações Anteriores

A organização mantém [Atribuição: versões anteriores definidas pela organização das configurações da linha de base do sistema de informações] para oferecer suporte à reversão.  
Guia Adicional: A retenção de versões anteriores das configurações da linha de base para oferecer suporte à reversão pode incluir, por exemplo, hardware, software, firmware, arquivos de configuração e registros de configuração.

### CM-2(4): Configuração Base de Referência | Software Não Autorizado

[Retirado: Incorporado ao CM-7].

### CM-2(5): Configuração Base de Referência | Software Autorizado

[Retirado: Incorporado ao CM-7].

### CM-2(6): Configuração Base de Referência | Desenvolvimento e Ambientes de Teste

A organização mantém uma configuração de linha de base para o desenvolvimento de sistemas de informação e ambientes de teste gerenciados separadamente da configuração da linha de base operacional.  
Guia Adicional: Estabelecer configurações de linha de base separadas para ambientes de desenvolvimento, teste e operacional ajuda a proteger os sistemas de informações de eventos não planejados / inesperados relacionados às atividades de desenvolvimento e teste. Configurações de linha de base separadas permitem que as organizações apliquem o gerenciamento de configuração mais apropriado para cada tipo de configuração. Por exemplo, o gerenciamento de configurações operacionais geralmente enfatiza a necessidade de estabilidade, enquanto o gerenciamento de configurações de desenvolvimento / teste requer maior flexibilidade. As configurações no ambiente de teste espelham as configurações no ambiente operacional na medida do possível, para que os resultados dos testes sejam representativos das alterações propostas nos sistemas operacionais. Esse aprimoramento de controle requer configurações separadas, mas não necessariamente ambientes físicos separados.

### CM-2(7): Configuração Base de Referência | Configurar Sistemas, Componentes ou Dispositivos para Áreas de Alto Risco

A organização:  
  
a. Emite [Atribuição: sistemas de informação, componentes ou dispositivos do sistema definidos pela organização] com [Atribuição: configurações definidas pela organização] a indivíduos que viajam para locais que a organização considera como de risco significativo; e  
  
b. Aplica [Atribuição: proteções de segurança definidas pela organização] aos dispositivos quando os indivíduos retornam.  
Guia Adicional: Quando se sabe que os sistemas de informação, componentes do sistema ou dispositivos (por exemplo, notebooks, dispositivos móveis) estarão localizados em áreas de alto risco, controles de segurança adicionais podem ser implementados para combater a maior ameaça nessas áreas, juntamente com a falta de segurança física relativa a áreas controladas pela organização. Por exemplo, políticas e procedimentos organizacionais para notebooks usados por indivíduos que partem e retornam de viagens incluem, por exemplo, determinar quais locais são preocupantes, definir as configurações necessárias para os dispositivos, garantir que os dispositivos sejam configurados conforme o planejado antes do início da viagem e aplicar salvaguardas específicas ao dispositivo após a conclusão da viagem. Os notebooks especialmente configurados incluem, por exemplo, computadores com discos rígidos higienizados, aplicativos limitados e proteção adicional (por exemplo, definições de configuração mais rigorosas). As salvaguardas especificadas aplicadas aos dispositivos móveis após o retorno da viagem incluem, por exemplo, examinar o dispositivo em busca de sinais de violação física e limpar/wipe a unidade de disco rígido. A proteção de informações residentes em dispositivos móveis é abordada na família de proteção de mídia.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-128 | https://csrc.nist.gov/publications/search?keywords-lg=800-128 |

## CM-3: Controle sobre Alterações de Configuração (P1)

**Descrição do Controle:**A organização:  
  
a. Determina os tipos de alterações no sistema de informação que são controladas por configuração;  
  
b. Analisa mudanças propostas, controladas por configuração, no sistema de informação e aprova ou desaprova essas mudanças, com consideração explícita das análises de impacto de segurança;  
  
c. A configuração de documentos altera decisões associadas ao sistema de informação;  
  
d. Implementa mudanças aprovadas controladas por configuração no sistema de informação;  
  
e. Retém registros de alterações controladas por configuração no sistema de informação para [Atribuição: período de tempo definido pela organização];  
  
f. Audita e revisa as atividades associadas a alterações controladas por configuração no sistema de informações; e  
  
g. Coordena e fornece supervisão para atividades de controle de mudança de configuração por meio de [Atribuição: elemento de controle de modificação da configuração definida pela organização (por exemplo, comitê, diretoria)] que convoca [Seleção (uma ou mais): [Atribuição: frequência definida pela organização]; [Atribuição: condições de mudança na configuração definida pela organização]].  
  
**Guia Adicional:**Controles de mudança de configuração para sistemas de informações organizacionais envolvem a proposta sistemática, justificativa, implementação, teste, revisão e disposição de mudanças nos sistemas, incluindo atualizações e modificações do sistema. O controle de alterações de configuração inclui alterações nas configurações de linha de base para componentes e itens de configuração de sistemas de informação, alterações nas configurações de produtos de tecnologia da informação (por exemplo, sistemas operacionais, aplicativos, firewalls, roteadores e dispositivos móveis), alterações não programadas / não autorizadas e alterações em corrigir vulnerabilidades. Processos típicos para gerenciar mudanças de configuração em sistemas de informação incluem, por exemplo, Placas de Controle de Configuração que aprovam mudanças propostas para sistemas. Para novos sistemas de informação de desenvolvimento ou sistemas submetidos a grandes atualizações, as organizações consideram a inclusão de representantes de organizações de desenvolvimento nos painéis de controle de configuração. A auditoria de mudanças inclui atividades antes e depois de mudanças nos sistemas de informações organizacionais e nas atividades de auditoria necessárias para implementar tais mudanças.  
  
**Melhorias do Controle:**

### CM-3(1): Controle sobre Alterações de Configuração | Documento Automatizado / Notificação / Proibição de Alterações

A organização emprega mecanismos automatizados para:  
  
a. Documente alterações propostas no sistema de informação;  
  
b. Notificar [Designação: autoridades de aprovação definidas] de alterações propostas no sistema de informações e solicitar aprovação de alterações;  
  
c. Destacar as alterações propostas ao sistema de informações que não foram aprovadas ou reprovadas por [Atribuição: período definido pela organização];  
  
d. Proibir alterações no sistema de informações até que as aprovações designadas sejam recebidas;  
  
e. Documente todas as alterações no sistema de informação; e  
  
f. Notifique [Atribuição: pessoal definido pela organização] quando as alterações aprovadas no sistema de informações forem concluídas.

### CM-3(2): Controle sobre Alterações de Configuração | Alterações de Teste / Validação / Documento

A organização testa, valida e documenta alterações no sistema de informações antes de implementar as alterações no sistema operacional.  
Guia Adicional: As alterações nos sistemas de informações incluem modificações nos componentes de hardware, software ou firmware e nas definições de configuração definidas no CM-6. As organizações garantem que o teste não interfira nas operações do sistema de informação. Os indivíduos / grupos que realizam testes compreendem as políticas e procedimentos de segurança organizacional, as políticas e procedimentos de segurança do sistema de informação e os riscos específicos de saúde, segurança e meio ambiente associados a instalações / processos específicos. Os sistemas operacionais podem precisar ser retirados da rede ou replicados na medida do possível, antes que o teste possa ser realizado. Se os sistemas de informação precisarem ser retirados da rede para teste, os testes estão programados para ocorrer durante interrupções planejadas do sistema, sempre que possível. Se o teste não puder ser realizado em sistemas operacionais, as organizações empregam controles compensadores (por exemplo, teste em sistemas replicados).

### CM-3(3): Controle sobre Alterações de Configuração | Implementação de Mudanças Automatizadas

A organização emprega mecanismos automatizados para implementar alterações na linha de base do sistema de informações atual e implanta a linha de base atualizada na base instalada.

### CM-3(4): Controle sobre Alterações de Configuração | Representante de Segurança

A organização exige que um representante de segurança da informação seja membro do [Atribuição: elemento de controle de alterações na configuração definida pela organização].  
Guia Adicional: Os representantes de segurança da informação podem incluir, por exemplo, agentes de segurança da informação da agência, oficiais de segurança do sistema de informação ou gerentes de segurança do sistema de informação. A representação por pessoal com experiência em segurança da informação é importante porque alterações nas configurações do sistema de informação podem ter efeitos colaterais indesejados, alguns dos quais podem ser relevantes para a segurança. A detecção de tais alterações no início do processo pode ajudar a evitar consequências indesejadas e negativas que podem afetar o estado de segurança dos sistemas de informações organizacionais. O elemento de controle de mudanças na configuração neste aprimoramento de controle reflete os elementos de controle de mudanças definidos pelas organizações no CM-3.

### CM-3(5): Controle sobre Alterações de Configuração | Resposta de Segurança Automatizada

O sistema de informações implementa [Atribuição: respostas de segurança definidas pela organização] automaticamente se as configurações da linha de base forem alteradas de maneira não autorizada.  
Guia Adicional: As respostas de segurança incluem, por exemplo, interromper o processamento do sistema de informações, interromper as funções selecionadas do sistema ou emitir alertas / notificações para a equipe organizacional quando houver uma modificação não autorizada de um item de configuração.

### CM-3(6): Controle sobre Alterações de Configuração | Gestão de Criptografia

A organização garante que os mecanismos criptográficos usados para fornecer [Atribuição: salvaguardas de segurança definidas pela organização] estejam sob gerenciamento de configuração.  
Guia Adicional: Independentemente dos meios criptográficos empregados (por exemplo, chave pública, chave privada, segredos compartilhados), as organizações garantem a existência de processos e procedimentos para gerenciar efetivamente esses meios. Por exemplo, se os dispositivos usam certificados como base para identificação e autenticação, é necessário que exista um processo para resolver a expiração desses certificados.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-128 | https://csrc.nist.gov/publications/search?keywords-lg=800-128 |

## CM-4: Análise de Impacto de Segurança (P2)

**Descrição do Controle:**A organização analisa as alterações no sistema de informações para determinar possíveis impactos na segurança antes de alterar a implementação.  
  
**Guia Adicional:**O pessoal organizacional com responsabilidades de segurança da informação (por exemplo, Administradores do Sistema de Informações, Oficiais de Segurança do Sistema de Informações, Gerentes de Segurança do Sistema de Informações e Engenheiros de Segurança do Sistema de Informações) conduz análises de impacto de segurança. Os indivíduos que realizam análises de impacto na segurança possuem as habilidades / conhecimentos técnicos necessários para analisar as alterações nos sistemas de informação e as ramificações de segurança associadas. A análise de impacto de segurança pode incluir, por exemplo, a revisão dos planos de segurança para entender os requisitos de controle de segurança e a análise da documentação de design do sistema para entender a implementação do controle e como alterações específicas podem afetar os controles. As análises de impacto na segurança também podem incluir avaliações de risco para entender melhor o impacto das alterações e determinar se são necessários controles de segurança adicionais. As análises de impacto na segurança são dimensionadas de acordo com as categorias de segurança dos sistemas de informação.  
  
**Melhorias do Controle:**

### CM-4(1): Análise de Impacto de Segurança | Ambientes de Ensaio Separados

A organização analisa as alterações no sistema de informações em um ambiente de teste separado antes da implementação em um ambiente operacional, procurando impactos na segurança devido a falhas, fraquezas, incompatibilidade ou malícia intencional.  
Guia Adicional: Ambiente de teste separado nesse contexto significa um ambiente fisicamente ou logicamente isolado e distinto do ambiente operacional. A separação é suficiente para garantir que as atividades no ambiente de teste não afetem as atividades no ambiente operacional e as informações no ambiente operacional não sejam transmitidas inadvertidamente ao ambiente de teste. Ambientes separados podem ser alcançados por meios físicos ou lógicos. Se ambientes de teste fisicamente separados não forem utilizados, as organizações determinarão a força do mecanismo necessário ao implementar a separação lógica (por exemplo, separação obtida por meio de máquinas virtuais).

### CM-4(2): Análise de Impacto de Segurança | Verificação de Funções de Segurança

A organização, após a alteração do sistema de informações, verifica as funções de segurança para verificar se as funções foram implementadas corretamente, operando conforme o planejado e produzindo o resultado desejado com relação ao atendimento dos requisitos de segurança do sistema.  
Guia Adicional: A implementação neste contexto refere-se à instalação de código alterado no sistema de informações operacionais.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-128 | https://csrc.nist.gov/publications/search?keywords-lg=800-128 |

## CM-5: Restrições de Acesso para Mudanças (P1)

**Descrição do Controle:**A organização define, documenta, aprova e impõe restrições de acesso físico e lógico associadas a alterações no sistema de informações.  
  
**Guia Adicional:**Quaisquer alterações nos componentes de hardware, software e/ou firmware dos sistemas de informação podem potencialmente ter efeitos significativos na segurança geral dos sistemas. Portanto, as organizações permitem que apenas indivíduos qualificados e autorizados acessem os sistemas de informações com o objetivo de iniciar mudanças, incluindo atualizações e modificações. As organizações mantêm registros de acesso para garantir que o controle de alterações na configuração seja implementado e para apoiar ações posteriores ao fato, caso as organizações descubram alterações não autorizadas. Restrições de acesso para mudança também incluem bibliotecas de software. As restrições de acesso incluem, por exemplo, controles de acesso físico e lógico (consulte AC-3 e PE-3), automação do fluxo de trabalho, bibliotecas de mídia, camadas abstratas (por exemplo, alterações implementadas em interfaces de terceiros e não diretamente nos sistemas de informações) e alterar janelas (por exemplo, as alterações ocorrem apenas durante períodos especificados, facilitando a descoberta de alterações não autorizadas).  
  
**Melhorias do Controle:**

### CM-5(1): Restrições de Acesso para Mudanças | Execução / Auditoria de Acesso Automatizado

O sistema de informações impõe restrições de acesso e suporta a auditoria das ações de imposição.

### CM-5(2): Restrições de Acesso para Mudanças | Revisão das Alterações do Sistema

A organização revisa as alterações no sistema de informações [Atribuição: frequência definida pela organização] e [Atribuição: circunstâncias definidas pela organização] para determinar se ocorreram alterações não autorizadas.  
Guia Adicional: Indicações que justificam a revisão das alterações do sistema de informações e as circunstâncias específicas que justificam essas revisões podem ser obtidas de atividades realizadas pelas organizações durante o processo de alteração da configuração.

### CM-5(3): Restrições de Acesso para Mudanças | Componentes Assinados

O sistema de informações impede a instalação de [Atribuição: componentes de software e firmware definidos pela organização] sem verificar se o componente foi assinado digitalmente usando um certificado que é reconhecido e aprovado pela organização.  
Guia Adicional: Os componentes de software e firmware impedidos de instalação, a menos que assinados com certificados reconhecidos e aprovados, incluem, por exemplo, atualizações de versão de software e firmware, patches, service packs, drivers de dispositivo e atualizações do BIOS (Basic Input Output System). As organizações podem identificar componentes de software e firmware aplicáveis por tipo, itens específicos ou uma combinação de ambos. As assinaturas digitais e a verificação organizacional de tais assinaturas são um método de autenticação de código.

### CM-5(4): Restrições de Acesso para Mudanças | Autorização Dupla

A organização aplica autorização dupla para implementar alterações em [Atribuição: componentes do sistema de informações definidas pela organização e informações em nível de sistema].  
Guia Adicional: As organizações empregam autorização dupla para garantir que quaisquer alterações nos componentes e informações selecionados do sistema de informações não possam ocorrer, a menos que dois indivíduos qualificados implementem essas alterações. Os dois indivíduos possuem habilidades / conhecimentos suficientes para determinar se as alterações propostas são implementações corretas das alterações aprovadas. A autorização dupla também pode ser conhecida como controle de duas pessoas.

### CM-5(5): Restrições de Acesso para Mudanças | Produção Limitada / Privilégios Operacionais

A organização:  
  
a. Limita os privilégios para alterar os componentes do sistema de informações e informações relacionadas ao sistema em um ambiente operacional ou de produção; e  
  
b. Revisa e reavalia privilégios [Atribuição: frequência definida pela organização].  
Guia Adicional: Em muitas organizações, os sistemas de informação suportam várias missões principais / funções de negócios. É necessário limitar os privilégios para alterar os componentes do sistema de informações em relação aos sistemas operacionais, pois as alterações em um componente específico do sistema de informações podem ter efeitos de longo alcance nos processos de missão / negócios suportados pelo sistema em que o componente reside. O complexo, muitos para muitos relacionamentos entre sistemas e processos de missão / negócios são, em alguns casos, desconhecidos pelos desenvolvedores.

### CM-5(6): Restrições de Acesso para Mudanças | Limitar Privilégios da Biblioteca

A organização limita os privilégios para alterar o software residente nas bibliotecas de software.  
Guia Adicional: As bibliotecas de software incluem programas privilegiados.

### CM-5(7): Restrições de Acesso para Mudanças | Implementação Automática De Salvaguardas De Segurança

[Retirado: Incorporado no SI-7].

## CM-6: Definições de Configuração (P1)

**Descrição do Controle:**A organização:  
  
a. Estabelece e documenta definições de configuração para produtos de tecnologia da informação empregados no sistema de informação usando [Atribuição: listas de verificação de configuração de segurança definidas pela organização] que refletem o modo mais restritivo consistente com os requisitos operacionais;  
  
b. Implementa as definições de configuração;  
  
c. Identifica, documenta e aprova quaisquer desvios das definições de configuração estabelecidas para [Atribuição: componentes do sistema de informações definidas pela organização] com base em [Atribuição: requisitos operacionais definidos pela organização]; e  
  
d. Monitora e controla as alterações nas configurações de acordo com as políticas e procedimentos organizacionais.  
  
**Guia Adicional:**Definições de configuração são o conjunto de parâmetros que podem ser alterados nos componentes de hardware, software ou firmware do sistema de informações que afetam a postura de segurança e/ou a funcionalidade do sistema. Os produtos de tecnologia da informação para os quais configurações de segurança podem ser definidas incluem, por exemplo, computadores mainframe, servidores (por exemplo, banco de dados, correio eletrônico, autenticação, web, proxy, arquivo, nome de domínio), estações de trabalho, dispositivos de entrada / saída scanners, copiadoras e impressoras), componentes de rede (por exemplo, firewalls, roteadores, gateways, comutadores de voz e dados, pontos de acesso sem fio, dispositivos de rede, sensores), sistemas operacionais, middleware e aplicativos. Parâmetros relacionados à segurança são aqueles parâmetros que afetam o estado de segurança dos sistemas de informação, incluindo os parâmetros necessários para satisfazer outros requisitos de controle de segurança. Parâmetros relacionados à segurança incluem, por exemplo: (i) configurações do registro; (ii) configurações de conta, arquivo, permissão de diretório; e (iii) configurações para funções, portas, protocolos, serviços e conexões remotas. As organizações estabelecem configurações de toda a organização e, subsequentemente, obtêm configurações específicas para sistemas de informação. As configurações estabelecidas tornam-se parte da linha de base da configuração de sistemas. Configurações seguras comuns (também conhecidas como listas de verificação de configuração de segurança, guias de bloqueio e proteção, guias de referência de segurança, guias de implementação técnica de segurança) fornecem referências reconhecidas, padronizadas e estabelecidas que estipulam configurações seguras para plataformas / produtos de tecnologia da informação específicos e instruções para configuração esses componentes do sistema de informações para atender aos requisitos operacionais. Configurações seguras comuns podem ser desenvolvidas por uma variedade de organizações, incluindo, por exemplo, desenvolvedores de produtos de tecnologia da informação, fabricantes, fornecedores, consórcios, academia, indústria, agências federais e outras organizações nos setores público e privado. Configurações seguras comuns incluem a Linha de Base de Configuração do Governo dos Estados Unidos (USGCB), que afeta a implementação do CM-6 e outros controles, como o AC-19 e o CM-7. O SCAP (Security Content Automation Protocol) e os padrões definidos dentro do protocolo (por exemplo, Common Configuration Enumeration) fornecem um método eficaz para identificar, rastrear e controlar as configurações de forma exclusiva. OMB estabelece política federal sobre requisitos de configuração para sistemas de informação federais.  
  
**Melhorias do Controle:**

### CM-6(1): Definições de Configuração | Gestão / Aplicação / Verificação Central Automatizada

A organização emprega mecanismos automatizados para gerenciar, aplicar e verificar centralmente as configurações de [Atribuição: componentes do sistema de informações definidas pela organização].

### CM-6(2): Definições de Configuração | Responder a Alterações Não Autorizadas

A organização emprega [Atribuição: salvaguardas de segurança definidas pela organização] para responder a alterações não autorizadas em [Atribuição: definições de configuração definidas pela organização].  
Guia Adicional: As respostas a alterações não autorizadas nas definições de configuração podem incluir, por exemplo, alertar a equipe organizacional designada, restaurar as definições estabelecidas ou, em casos extremos, interromper o processamento do sistema de informações afetado.

### CM-6(3): Definições de Configuração | Detecção de Mudanças Não Autorizada

[Retirado: Incorporado no SI-7].

### CM-6(4): Definições de Configuração | Demonstração de Conformidade

[Retirado: Incorporado ao CM-4].

**Referências:**

|  |  |
| --- | --- |
| OMB Memorando 07-11 | https://georgewbush-whitehouse.archives.gov/omb/memoranda/fy2007/m07-11.pdf |
| OMB Memorando 07-18 | https://georgewbush-whitehouse.archives.gov/omb/memoranda/fy2007/m07-18.pdf |
| OMB Memorando 08-22 | https://georgewbush-whitehouse.archives.gov/omb/memoranda/fy2008/m08-22.pdf |
| Publicação Especial NIST 800-70 | https://csrc.nist.gov/publications/search?keywords-lg=800-70 |
| Publicação Especial NIST 800-128 | https://csrc.nist.gov/publications/search?keywords-lg=800-128 |
| NIST - NVD: Banco de Dados Nacional de Vulnerabilidades | http://nvd.nist.gov |
| NIST - Checklists | http://checklists.nist.gov |
| NSA: Agência Nacional de Segurança | http://www.nsa.gov |

## CM-7: Menor Funcionalidade (P1)

**Descrição do Controle:**A organização:  
  
a. Configura o sistema de informações para fornecer apenas recursos essenciais; e  
  
b. Proíbe ou restringe o uso das seguintes funções, portas, protocolos e/ou serviços: [Atribuição: funções proibidas ou restritas definidas pela organização, portas, protocolos e/ou serviços].  
  
**Guia Adicional:**Os sistemas de informação podem fornecer uma ampla variedade de funções e serviços. Algumas das funções e serviços, fornecidos por padrão, podem não ser necessários para suportar operações organizacionais essenciais (por exemplo, missões-chave, funções). Além disso, às vezes é conveniente fornecer vários serviços a partir de componentes do sistema de informações único, mas isso aumenta o risco de limitar os serviços fornecidos por qualquer componente. Sempre que possível, as organizações limitam a funcionalidade dos componentes a uma única função por dispositivo (por exemplo, servidores de e-mail ou servidores da Web, mas não ambos). Organizações revisam funções e serviços fornecidos por sistemas de informação ou componentes individuais de sistemas de informação, para determinar quais funções e serviços são candidatos à eliminação (por exemplo, Voice Over Internet Protocol, Mensagens Instantâneas, auto execução e compartilhamento de arquivos). As organizações consideram a desativação de portas / protocolos físicos e lógicos não utilizados ou desnecessários (por exemplo, Universal Serial Bus, File Transfer Protocol e Hyper Text Transfer Protocol) nos sistemas de informação para impedir a conexão não autorizada de dispositivos, a transferência não autorizada de informações ou o tunelamento não autorizado. As organizações podem utilizar ferramentas de varredura de rede, sistemas de detecção e prevenção de intrusões e proteções de ponto final, como firewalls e sistemas de detecção de intrusões baseados em host, para identificar e impedir o uso de funções, portas, protocolos e serviços proibidos.  
  
**Melhorias do Controle:**

### CM-7(1): Menor Funcionalidade | Revisão Periódica

A organização:  
  
a. Revisa o sistema de informações [Atribuição: frequência definida pela organização] para identificar funções, portas, protocolos e serviços desnecessários e/ou não seguros; e  
  
b. Desativa [Atribuição: funções, portas, protocolos e serviços definidos pela organização no sistema de informações considerados desnecessários e/ou não seguros].  
Guia Adicional: A organização pode determinar a segurança relativa da função, porta, protocolo e/ou serviço ou basear a decisão de segurança na avaliação de outras entidades. Bluetooth, FTP e redes ponto a ponto são exemplos de protocolos menos que seguros.

### CM-7(2): Menor Funcionalidade | Impedir a Execução do Programa

O sistema de informações impede a execução do programa de acordo com [Seleção (uma ou mais): [Atribuição: políticas definidas pela organização em relação ao uso e restrições de programas de software]; regras que autorizam os termos e condições de uso do programa de software].

### CM-7(3): Menor Funcionalidade | Conformidade com Inscrição

A organização garante a conformidade com [Atribuição: requisitos de registro definidos pela organização para funções, portas, protocolos e serviços].  
Guia Adicional: As organizações usam o processo de registro para gerenciar, rastrear e supervisionar sistemas de informação e funções, portas, protocolos e serviços implementados.

### CM-7(4): Menor Funcionalidade | Software Não Autorizado / Lista Negra

A organização:  
  
a. Identifica [Atribuição: programas de software definidos pela organização não autorizados a executar no sistema de informação];  
  
b. Emprega uma política de permitir tudo, negar por exceção para proibir a execução de programas de software não autorizados no sistema de informações; e  
  
c. Revisa e atualiza a lista de programas de software não autorizados [Atribuição: frequência definida pela organização].  
Guia Adicional: O processo usado para identificar programas de software que não estão autorizados a executar em sistemas de informações organizacionais é geralmente chamado de lista negra. As organizações podem implementar o CM-7 (5) em vez desse aprimoramento de controle se a lista de permissões (a mais forte das duas políticas) for a abordagem preferida para restringir a execução de programas de software.

### CM-7(5): Menor Funcionalidade | Software Autorizado / Lista Branca

A organização:  
  
a. Identifica [Atribuição: programas de software definidos pela organização, autorizados a executar no sistema de informação];  
  
b. Emprega uma política de negar tudo, permitir por exceção, para permitir a execução de programas de software autorizados no sistema de informação; e  
  
c. Revisa e atualiza a lista de programas de software autorizados [Atribuição: frequência definida pela organização].  
Guia Adicional: O processo usado para identificar programas de software que estão autorizados a executar em sistemas de informações organizacionais é geralmente chamado de lista de permissões. Além da lista de permissões, as organizações consideram verificar a integridade de programas de software listados usando, por exemplo, somas de verificação criptográficas, assinaturas digitais ou funções de hash. A verificação do software listado em branco pode ocorrer antes da execução ou na inicialização do sistema.

**Referências:**

|  |  |
| --- | --- |
| Instruções do Departamento de Defesa dos EUA N.8551.01 | https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/855101p.pdf |

## CM-8: Inventário de Componentes do Sistema (P1)

**Descrição do Controle:**A organização:  
  
a. Desenvolve e documenta um inventário de componentes do sistema de informação que:  
  
1. Reflete com precisão o sistema de informação atual;  
  
2. Inclui todos os componentes dentro dos limites de autorização do sistema de informação;  
  
3. Está no nível de granularidade considerado necessário para rastreamento e relatório; e  
  
4. Inclui [Atribuição: informação definida pela organização considerada necessária para conseguir uma prestação de contas eficaz do componente do sistema de informação]; e  
  
b. Revisa e atualiza o inventário de componentes do sistema de informações [Atribuição: frequência definida pela organização].  
  
**Guia Adicional:**As organizações podem optar por implementar inventários de componentes centralizados do sistema de informações que incluam componentes de todos os sistemas de informações organizacionais. Em tais situações, as organizações garantem que os inventários resultantes incluam informações específicas do sistema necessárias para a responsabilidade adequada do componente (por exemplo, associação do sistema de informações, proprietário do sistema de informações). As informações consideradas necessárias para a responsabilidade efetiva dos componentes do sistema de informações incluem, por exemplo, especificações de inventário de hardware, informações de licença de software, números de versão de software, proprietários de componentes e componentes ou dispositivos em rede, nomes de máquinas e endereços de rede. As especificações de inventário incluem, por exemplo, fabricante, tipo de dispositivo, modelo, número de série e localização física.  
  
**Melhorias do Controle:**

### CM-8(1): Inventário de Componentes do Sistema | Atualizações Durante as Instalações / Remoções

A organização atualiza o inventário dos componentes do sistema de informações como parte integrante das instalações, remoções e atualizações do sistema de componentes.

### CM-8(2): Inventário de Componentes do Sistema | Manutenção Automatizada

A organização emprega mecanismos automatizados para ajudar a manter um inventário atualizado, completo, preciso e prontamente disponível dos componentes do sistema de informação.  
Guia Adicional: As organizações mantêm inventários de sistemas de informação na medida do possível. Máquinas virtuais, por exemplo, podem ser difíceis de monitorar, porque não são visíveis para a rede quando não estão em uso. Nesses casos, as organizações mantêm um inventário atualizado, completo e preciso, conforme considerado razoável. Esse aprimoramento de controle pode ser satisfeito com a implementação do CM-2 (2) para organizações que optam por combinar o inventário de componentes do sistema de informações e as atividades de configuração da linha de base.

### CM-8(3): Inventário de Componentes do Sistema | Detecção Automática Não Autorizada de Componentes

A organização:  
  
a. Emprega mecanismos automatizados [Atribuição: frequência definida pela organização] para detectar a presença de componentes não autorizados de hardware, software e firmware no sistema de informação; e  
  
b. Executa as seguintes ações quando são detectados componentes não autorizados: [Seleção (um ou mais): desativa o acesso à rede por esses componentes; isola os componentes; notifica [Atribuição: pessoal ou funções definidas pela organização]].  
Guia Adicional: Esse aprimoramento de controle é aplicado além do monitoramento de conexões remotas não autorizadas e dispositivos móveis. O monitoramento de componentes não autorizados do sistema pode ser realizado continuamente ou pela verificação periódica dos sistemas para esse fim. Mecanismos automatizados podem ser implementados dentro de sistemas de informação ou em outros dispositivos separados. O isolamento pode ser alcançado, por exemplo, colocando componentes não autorizados do sistema de informações em domínios ou sub-redes separados ou colocando em quarentena esses componentes. Esse tipo de isolamento de componente é geralmente chamado de sandboxing.

### CM-8(4): Inventário de Componentes do Sistema | Informação sobre Responsabilidade

A organização inclui no sistema, informações de inventário de componentes, um meio para identificar por [Seleção (um ou mais): nome; posição; função], indivíduos responsáveis / responsáveis pela administração desses componentes.  
Guia Adicional: A identificação de indivíduos responsáveis e responsáveis pela administração dos componentes do sistema de informações ajuda a garantir que os componentes atribuídos sejam administrados adequadamente e as organizações possam entrar em contato com esses indivíduos se alguma ação for necessária (por exemplo, um componente é considerado a fonte de uma violação / comprometimento, componente precisa ser recuperado / substituído ou componente precisa ser realocado).

### CM-8(5): Inventário de Componentes do Sistema | Nenhuma Conta Duplicada de Componentes

A organização verifica se todos os componentes dentro do limite de autorização do sistema de informação não estão duplicados em outros inventários de componentes do sistema de informação.  
Guia Adicional: Esse aprimoramento de controle aborda o problema potencial da contabilidade duplicada dos componentes do sistema de informações em sistemas interconectados grandes ou complexos.

### CM-8(6): Inventário de Componentes do Sistema | Configurações Avaliadas / Desvios Aprovados

A organização inclui configurações de componentes avaliadas e quaisquer desvios aprovados para as configurações implementadas atualmente no inventário de componentes do sistema de informações.  
Guia Adicional: Esse aprimoramento de controle concentra-se nas definições de configuração estabelecidas pelas organizações para os componentes do sistema de informações, os componentes específicos que foram avaliados para determinar a conformidade com as definições de configuração necessárias e quaisquer desvios aprovados das definições de configuração estabelecidas.

### CM-8(7): Inventário de Componentes do Sistema | Repositório Centralizado

A organização fornece um repositório centralizado para o inventário dos componentes do sistema de informação.  
Guia Adicional: As organizações podem optar por implementar inventários de componentes centralizados do sistema de informações que incluam componentes de todos os sistemas de informações organizacionais. Repositórios centralizados de inventários de componentes de sistemas de informações oferecem oportunidades de eficiência na contabilização de ativos de hardware, software e firmware organizacionais. Esses repositórios também podem ajudar as organizações a identificar rapidamente o local e os indivíduos responsáveis pelos componentes do sistema que foram comprometidos, violados ou que precisam de ações de mitigação. As organizações garantem que os inventários centralizados resultantes incluam informações específicas do sistema, necessárias para a responsabilização adequada dos componentes (por exemplo, associação do sistema de informações, proprietário do sistema de informações).

### CM-8(8): Inventário de Componentes do Sistema | Rastreamento de Localização Automatizado

A organização emprega mecanismos automatizados para oferecer suporte ao rastreamento dos componentes do sistema de informações por localização geográfica.  
Guia Adicional: O uso de mecanismos automatizados para rastrear a localização dos componentes do sistema de informações pode aumentar a precisão dos inventários de componentes. Essa capacidade também pode ajudar as organizações a identificar rapidamente o local e os indivíduos responsáveis pelos componentes do sistema que foram comprometidos, violados ou que precisam de ações de mitigação.

### CM-8(9): Inventário de Componentes do Sistema | Atribuição de Componentes a Sistemas

A organização:  
  
a. Atribui [Atribuição: componentes do sistema de informações adquiridas definidos pela organização] a um sistema de informações; e  
  
b. Recebe uma confirmação do proprietário do sistema de informações desta atribuição  
Guia Adicional: As organizações determinam os critérios ou tipos de componentes do sistema de informações (por exemplo, microprocessadores, placas mãe, software, controladores lógicos programáveis e dispositivos de rede) que estão sujeitos a esse aprimoramento de controle.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-128 | https://csrc.nist.gov/publications/search?keywords-lg=800-128 |

## CM-9: Plano de Gerenciamento de Configuração (P1)

**Descrição do Controle:**A organização desenvolve, documenta e implementa um plano de gerenciamento de configuração para o sistema de informações que:  
  
a. Aborda funções, responsabilidades e processos e procedimentos de gerenciamento de configuração;  
  
b. Estabelece um processo para identificar itens de configuração ao longo do ciclo de vida de desenvolvimento do sistema e para gerenciar a configuração dos itens de configuração;  
  
c. Define os itens de configuração para o sistema de informações e coloca os itens de configuração no gerenciamento de configuração; e  
  
d. Protege o plano de gerenciamento de configuração contra divulgação e modificação não autorizadas.  
  
**Guia Adicional:**Os planos de gerenciamento de configuração atendem aos requisitos das políticas de gerenciamento de configuração, sendo adaptados aos sistemas de informações individuais. Esses planos definem processos e procedimentos detalhados sobre como o gerenciamento de configuração é usado para dar suporte às atividades do ciclo de vida de desenvolvimento do sistema no nível do sistema de informações. Os planos de gerenciamento de configuração são normalmente desenvolvidos durante a fase de desenvolvimento / aquisição do ciclo de vida de desenvolvimento do sistema. Os planos descrevem como mover mudanças através dos processos de gerenciamento de mudanças, como atualizar configurações e linhas de base, como manter os inventários de componentes do sistema de informações, como controlar o desenvolvimento, teste e ambientes operacionais, e como desenvolver, liberar e atualizar documentos importantes. As organizações podem empregar modelos para ajudar a garantir o desenvolvimento e a implementação consistentes e oportunos dos planos de gerenciamento de configuração. Esses modelos podem representar um plano de gerenciamento de configuração principal para a organização como um todo, com subconjuntos do plano implementados em um sistema por sistema. Os processos de aprovação de gerenciamento de configuração incluem a designação de partes interessadas no gerenciamento de chaves responsáveis por revisar e aprovar as alterações propostas aos sistemas de informação e o pessoal que conduz as análises de impacto de segurança antes da implementação de alterações nos sistemas. Itens de configuração são itens do sistema de informações (hardware, software, firmware e documentação) a serem gerenciados pela configuração. À medida que os sistemas de informação continuam durante o ciclo de vida de desenvolvimento do sistema, novos itens de configuração podem ser identificados e alguns itens de configuração existentes podem não precisar mais estar sob controle de configuração.  
  
**Melhorias do Controle:**

### CM-9(1): Plano de Gerenciamento de Configuração | Cessão de Responsabilidade

A organização atribui a responsabilidade pelo desenvolvimento do processo de gerenciamento de configuração à equipe organizacional que não está diretamente envolvida no desenvolvimento do sistema de informações.  
Guia Adicional: Na ausência de equipes dedicadas de gerenciamento de configuração atribuídas nas organizações, os desenvolvedores do sistema podem ser encarregados de desenvolver processos de gerenciamento de configuração usando pessoal que não esteja diretamente envolvido no desenvolvimento ou integração do sistema. Essa separação de tarefas garante que as organizações estabeleçam e mantenham um grau suficiente de independência entre os processos de desenvolvimento e integração de sistemas de informação e os processos de gerenciamento de configurações para facilitar o controle de qualidade e a supervisão mais eficaz.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-128 | https://csrc.nist.gov/publications/search?keywords-lg=800-128 |

## CM-10: Restrições de Uso do Software (P2)

**Descrição do Controle:**A organização:  
  
a. Usa software e documentação associada de acordo com contratos e leis de direitos autorais;  
  
b. Rastreia o uso de software e documentação associada protegidos por licenças de quantidade para controlar a cópia e a distribuição; e  
  
c. Controla e documenta o uso da tecnologia de compartilhamento de arquivos ponto a ponto para garantir que esse recurso não seja usado para distribuição, exibição, desempenho ou reprodução não autorizados de trabalhos protegidos por direitos autorais.  
  
**Guia Adicional:**O rastreamento de licenças de software pode ser realizado por métodos manuais (por exemplo, planilhas simples) ou métodos automatizados (por exemplo, aplicativos de rastreamento especializados), dependendo das necessidades da organização.  
  
**Melhorias do Controle:**

### CM-10(1): Restrições de Uso do Software | Software Livre (Open Source)

A organização estabelece as seguintes restrições ao uso de software de código aberto: [Atribuição: restrições definidas pela organização].  
Guia Adicional: Software de código aberto refere-se ao software disponível no formato de código-fonte. Certos direitos de software normalmente reservados para detentores de direitos autorais são rotineiramente fornecidos sob contratos de licença de software que permitem que indivíduos estudem, alterem e melhorem o software. Do ponto de vista da segurança, a principal vantagem do software de código aberto é que ele fornece às organizações a capacidade de examinar o código-fonte. No entanto, também existem vários problemas de licenciamento associados ao software de código aberto, incluindo, por exemplo, as restrições ao uso derivado desse software.

## CM-11: Software Instalado pelo Usuário (P1)

**Descrição do Controle:**A organização:  
  
a. Estabelece [Atribuição: políticas definidas pela organização] que regem a instalação de software pelos usuários;  
  
b. Impõe políticas de instalação de software através de [Atribuição: métodos definidos pela organização]; e  
  
b. Monitora a conformidade com a política em [Atribuição: frequência definida pela organização].  
  
**Guia Adicional:**Se tiverem os privilégios necessários, os usuários poderão instalar software em sistemas de informações organizacionais. Para manter o controle sobre os tipos de software instalados, as organizações identificam ações permitidas e proibidas relacionadas à instalação do software. As instalações de software permitidas podem incluir, por exemplo, atualizações e patches de segurança para o software existente e o download de aplicativos de "lojas de aplicativos" aprovadas pela organização. As instalações de software proibidas podem incluir, por exemplo, software com linhagem desconhecida ou suspeita ou software que as organizações considerem potencialmente malicioso. As organizações de políticas selecionadas que governam o software instalado pelo usuário podem ser desenvolvidas pela organização ou fornecidas por alguma entidade externa. Os métodos de imposição de políticas incluem métodos processuais (por exemplo, exame periódico das contas do usuário), métodos automatizados (por exemplo, configurações implementadas em sistemas de informações organizacionais) ou ambos.  
  
**Melhorias do Controle:**

### CM-11(1): Software Instalado pelo Usuário | Alertas para Instalações Não Autorizadas

O sistema de informações alerta [Designação: pessoal ou funções definidas pela organização] quando a instalação não autorizada de software é detectada.

### CM-11(2): Software Instalado pelo Usuário | Proibir a Instalação Sem Estado Privilegiado

O sistema de informações proíbe a instalação do software pelo usuário sem status privilegiado explícito.  
Guia Adicional: O status privilegiado pode ser obtido, por exemplo, atuando na função de administrador do sistema.

# CP - Planejamento de Contingência

## CP-1: Política e Procedimentos do Planeamento de Contingência (P1)

**Descrição do Controle:**A organização:  
  
a. Desenvolve, documenta e dissemina para [Atribuição: pessoal ou funções definidas pela organização]:  
  
1. Uma política de planejamento de contingência que trata da finalidade, escopo, funções, responsabilidades, compromisso de gerenciamento, coordenação entre entidades organizacionais e conformidade; e  
  
2. Procedimentos para facilitar a implementação da política de planejamento de contingência e controles de planejamento de contingência associados; e  
  
b. Analisa e atualiza a atual:  
  
1. Política de planejamento de contingência [Atribuição: frequência definida pela organização]; e  
  
2. Procedimentos de planejamento de contingência [Atribuição: frequência definida pela organização].  
  
**Guia Adicional:**Esse controle aborda o estabelecimento de políticas e procedimentos para a implementação efetiva de controles de segurança selecionados e aprimoramentos de controle na família CP. As políticas e procedimentos refletem as leis federais aplicáveis, ordens executivas, diretivas, regulamentos, políticas, normas e diretrizes. Políticas e procedimentos do programa de segurança no nível da organização podem tornar desnecessária a necessidade de políticas e procedimentos específicos do sistema. A política pode ser incluída como parte da política geral de segurança da informação para organizações ou, inversamente, pode ser representada por múltiplas políticas refletindo a natureza complexa de certas organizações. Os procedimentos podem ser estabelecidos para o programa de segurança em geral e para sistemas de informação específicos, se necessário. A estratégia de gerenciamento de risco organizacional é um fator chave no estabelecimento de políticas e procedimentos.

**Referências:**

|  |  |
| --- | --- |
| Diretiva de Continuidade Federal 1 | https://www.fema.gov/media-library-data/1486472423990-f640b42b9073d78693795bb7da4a7af2/January2017FCD1.pdf |
| Publicação Especial NIST 800-12 | https://csrc.nist.gov/publications/search?keywords-lg=800-12 |
| Publicação Especial NIST 800-34 | https://csrc.nist.gov/publications/search?keywords-lg=800-34 |
| Publicação Especial NIST 800-100 | https://csrc.nist.gov/publications/search?keywords-lg=800-100 |

## CP-2: Plano de Contingência (P1)

**Descrição do Controle:**A organização:  
  
a. Desenvolve um plano de contingência para o sistema de informação que:  
  
1. Identifica missões essenciais e funções de negócios e requisitos de contingência associados;  
  
2. Fornece objetivos de recuperação, prioridades de restauração e métricas;  
  
3. Aborda papéis de contingência, responsabilidades, indivíduos designados com informações de contato;  
  
4. Aborda a manutenção de missões e funções comerciais essenciais, apesar de uma interrupção, comprometimento ou falha do sistema de informação;  
  
5. Aborda eventual restauração completa do sistema de informações sem deteriorar as salvaguardas de segurança originalmente planejadas e implementadas; e  
  
6. É revisado e aprovado por [Designação: pessoal ou funções definidas pela organização];  
  
b. Distribui cópias do plano de contingência para [Atribuição: pessoal-chave de contingência definido pela organização (identificado por nome e/ou função) e elementos organizacionais];  
  
c. Coordena atividades de planejamento de contingência com atividades de tratamento de incidentes;  
  
d. Revisa o plano de contingência para o sistema de informações [Atribuição: frequência definida pela organização];  
  
e. Atualiza o plano de contingência para tratar de alterações na organização, sistema de informações ou ambiente de operação e problemas encontrados durante a implementação, execução ou teste do plano de contingência;  
  
f. Comunica alterações no plano de contingência para [Atribuição: pessoal-chave de contingência definido pela organização (identificado por nome e/ou função) e elementos organizacionais]; e  
  
g. Protege o plano de contingência contra divulgação e modificação não autorizadas.  
  
**Guia Adicional:**O planejamento de contingência para sistemas de informação é parte de um programa organizacional geral para obter continuidade de operações para funções de missão / negócios. O planejamento de contingência aborda a restauração do sistema de informações e a implementação de processos alternativos de missão / negócios quando os sistemas são comprometidos. A eficácia do planejamento de contingência é maximizada considerando esse planejamento ao longo das fases do ciclo de vida de desenvolvimento do sistema. A execução de planejamento de contingência no desenvolvimento de hardware, software e firmware pode ser um meio eficaz de obter resiliência do sistema de informações. Os planos de contingência refletem o grau de restauração necessário para os sistemas de informações organizacionais, pois nem todos os sistemas precisam se recuperar totalmente para atingir o nível de continuidade das operações desejadas. Os objetivos de recuperação do sistema de informações refletem as leis, ordens executivas, diretrizes, políticas, normas, regulamentos e diretrizes aplicáveis. Além da disponibilidade do sistema de informações, os planos de contingência também abordam outros eventos relacionados à segurança, resultando em uma redução na missão e/ou na eficácia dos negócios, como ataques maliciosos que comprometem a confidencialidade ou a integridade dos sistemas de informação. As ações abordadas nos planos de contingência incluem, por exemplo, degradação ordenada / normal, desligamento do sistema de informações, retorno ao modo manual, fluxos de informações alternativos e operação nos modos reservados para quando os sistemas estão sob ataque. Ao coordenar de perto o planejamento de contingência com as atividades de tratamento de incidentes, as organizações podem garantir que as atividades de planejamento de contingência necessárias estejam implementadas e ativadas no caso de um incidente de segurança.  
  
**Melhorias do Controle:**

### CP-2(1): Plano de Contingência | Coordenar com Planos Relacionados

A organização coordena o desenvolvimento do plano de contingência com os elementos organizacionais responsáveis pelos planos relacionados.  
Guia Adicional: Os planos relacionados aos planos de contingência para sistemas de informações organizacionais incluem, por exemplo, Planos de Continuidade de Negócios, Planos de Recuperação de Desastres, Planos de Continuidade de Operações, Planos de Comunicação de Crise, Planos de Infraestrutura Crítica, Planos de Resposta a Cyber Incidentes, Plano de Implementação de Ameaças Internas e Planos de Emergência para Ocupantes.

### CP-2(2): Plano de Contingência | Planejamento de Capacidade

A organização realiza o planejamento da capacidade para que exista a capacidade necessária para processamento de informações, telecomunicações e suporte ambiental durante as operações de contingência.  
Guia Adicional: O planejamento da capacidade é necessário porque diferentes tipos de ameaças (por exemplo, desastres naturais, ataques cibernéticos direcionados) podem resultar em uma redução dos serviços de processamento, telecomunicações e suporte disponíveis, originalmente destinados a apoiar as missões organizacionais / funções de negócios. As organizações podem precisar antecipar operações degradadas durante operações de contingência e fatorar essa degradação no planejamento da capacidade.

### CP-2(3): Plano de Contingência | Retomar Missões Essenciais / Funções de Negócio

A organização planeja a retomada de missões essenciais e funções de negócios dentro de [Atribuição: período definido pela organização] da ativação do plano de contingência.  
Guia Adicional: As organizações podem optar por realizar as atividades de planejamento de contingência nesse aprimoramento de controle como parte do planejamento organizacional de continuidade de negócios, incluindo, por exemplo, como parte das análises de impacto nos negócios. O período para a retomada de missões essenciais / funções de negócios pode depender da gravidade / extensão das interrupções no sistema de informações e em sua infraestrutura de suporte.

### CP-2(4): Plano de Contingência | Retomar Todas as Missões / Funções de Negócio

A organização planeja a retomada de todas as missões e funções de negócios dentro de [Atribuição: período definido pela organização] da ativação do plano de contingência.  
Guia Adicional: As organizações podem optar por realizar as atividades de planejamento de contingência nesse aprimoramento de controle como parte do planejamento organizacional de continuidade de negócios, incluindo, por exemplo, como parte das análises de impacto nos negócios. O período de tempo para a retomada de todas as missões / funções comerciais pode depender da gravidade / extensão das interrupções no sistema de informações e em sua infraestrutura de suporte.

### CP-2(5): Plano de Contingência | Continuidade de Missões Essenciais / Funções de Negócio

A organização planeja a continuidade de missões essenciais e funções de negócios com pouca ou nenhuma perda de continuidade operacional e mantém essa continuidade até a restauração completa do sistema de informações nos principais locais de processamento e/ou armazenamento.  
Guia Adicional: As organizações podem optar por realizar as atividades de planejamento de contingência nesse aprimoramento de controle como parte do planejamento organizacional de continuidade de negócios, incluindo, por exemplo, como parte das análises de impacto nos negócios. Os sites de processamento e/ou armazenamento primário definidos pelas organizações como parte do planejamento de contingência podem mudar dependendo das circunstâncias associadas à contingência (por exemplo, sites de backup podem se tornar sites primários).

### CP-2(6): Plano de Contingência | Local Alternativo de Processamento / Armazenamento

A organização planeja a transferência de missões essenciais e funções de negócios para alternar locais de processamento e/ou armazenamento com pouca ou nenhuma perda de continuidade operacional e sustenta essa continuidade através da restauração do sistema de informações nos locais principais de processamento e/ou armazenamento.  
Guia Adicional: As organizações podem optar por realizar as atividades de planejamento de contingência nesse aprimoramento de controle como parte do planejamento organizacional de continuidade de negócios, incluindo, por exemplo, como parte das análises de impacto nos negócios. Os sites de processamento e/ou armazenamento primário definidos pelas organizações como parte do planejamento de contingência podem mudar dependendo das circunstâncias associadas à contingência (por exemplo, sites de backup podem se tornar sites primários).

### CP-2(7): Plano de Contingência | Coordenar com Prestadores de Serviços Externos

A organização coordena seu plano de contingência com os planos de contingência de prestadores de serviços externos para garantir que os requisitos de contingência possam ser atendidos.  
Guia Adicional: Quando a capacidade de uma organização de executar com êxito suas principais missões / funções de negócios depende de prestadores de serviços externos, o desenvolvimento de um plano de contingência oportuno e abrangente pode se tornar mais desafiador. Nessa situação, as organizações coordenam as atividades de planejamento de contingência com as entidades externas para garantir que os planos individuais reflitam as necessidades gerais de contingência da organização.

### CP-2(8): Plano de Contingência | Identificar Ativos Críticos

A organização identifica ativos críticos do sistema de informações que dão suporte a missões essenciais e funções de negócios.  
Guia Adicional: As organizações podem optar por realizar as atividades de planejamento de contingência nesse aprimoramento de controle como parte do planejamento organizacional de continuidade de negócios, incluindo, por exemplo, como parte das análises de impacto nos negócios. As organizações identificam ativos críticos do sistema de informações para que salvaguardas e contramedidas adicionais possam ser empregadas (acima e além dessas salvaguardas e contramedidas implementadas rotineiramente) para ajudar a garantir que as missões organizacionais / funções de negócios possam continuar sendo realizadas durante operações de contingência. Além disso, a identificação de ativos de informações críticas facilita a priorização de recursos organizacionais. Os ativos críticos do sistema de informações incluem aspectos técnicos e operacionais. Os aspectos técnicos incluem, por exemplo, serviços de tecnologia da informação, componentes de sistemas de informação, produtos e mecanismos de tecnologia da informação. Os aspectos operacionais incluem, por exemplo, procedimentos (operações executadas manualmente) e pessoal (indivíduos que operam salvaguardas técnicas e/ou executam procedimentos manuais). Os planos de proteção de programas organizacionais podem fornecer assistência na identificação de ativos críticos.

**Referências:**

|  |  |
| --- | --- |
| Diretiva de Continuidade Federal 1 | https://www.fema.gov/media-library-data/1486472423990-f640b42b9073d78693795bb7da4a7af2/January2017FCD1.pdf |
| Publicação Especial NIST 800-34 | https://csrc.nist.gov/publications/search?keywords-lg=800-34 |

## CP-3: Treinamento de Contingência (P2)

**Descrição do Controle:**A organização fornece treinamento de contingência para os usuários do sistema de informação de acordo com as funções e responsabilidades atribuídas:  
  
a. Dentro de [Atribuição: período definido pela organização] de assumir uma função ou responsabilidade de contingência;  
  
b. Quando exigido pelas alterações do sistema de informação; e  
  
c. [Atribuição: frequência definida-organização] depois.  
  
**Guia Adicional:**O treinamento de contingência fornecido pelas organizações está vinculado às funções e responsabilidades atribuídas do pessoal da organização para garantir que o conteúdo e o nível de detalhes apropriados sejam incluídos nesse treinamento. Por exemplo, usuários regulares podem apenas precisar saber quando e onde relatar suas obrigações durante operações de contingência e se as obrigações normais são afetadas; os administradores do sistema podem exigir treinamento adicional sobre como configurar sistemas de informação em sites de processamento e armazenamento alternativos; e os gerentes / líderes seniores podem receber treinamento mais específico sobre como conduzir funções essenciais à missão em locais designados fora do local e como estabelecer comunicações com outras entidades governamentais para fins de coordenação de atividades relacionadas à contingência. O treinamento para papéis / responsabilidades de contingência reflete os requisitos específicos de continuidade no plano de contingência.  
  
**Melhorias do Controle:**

### CP-3(1): Treinamento de Contingência | Eventos Simulados

A organização incorpora eventos simulados ao treinamento de contingência para facilitar a resposta eficaz do pessoal em situações de crise.

### CP-3(2): Treinamento de Contingência | Ambientes Automatizados de Formação

A organização emprega mecanismos automatizados para fornecer um ambiente de treinamento de contingência mais completo e realista.

**Referências:**

|  |  |
| --- | --- |
| Diretiva de Continuidade Federal 1 | https://www.fema.gov/media-library-data/1486472423990-f640b42b9073d78693795bb7da4a7af2/January2017FCD1.pdf |
| Publicação Especial NIST 800-16 | https://csrc.nist.gov/publications/search?keywords-lg=800-16 |
| Publicação Especial NIST 800-50 | https://csrc.nist.gov/publications/search?keywords-lg=800-50 |

## CP-4: Teste do Plano de Contingência (P2)

**Descrição do Controle:**A organização:  
  
a. Testa o plano de contingência para o sistema de informação [Atribuição: frequência definida pela organização] usando [Atribuição: testes definidos pela organização] para determinar a eficácia do plano e a prontidão organizacional para executar o plano;  
  
b. Revisa os resultados dos testes do plano de contingência; e  
  
c. Inicia ações corretivas, se necessário.  
  
**Guia Adicional:**Os métodos para testar os planos de contingência para determinar a eficácia dos planos e para identificar possíveis fraquezas nos planos incluem, por exemplo, exercícios de walkthrough e de mesa, listas de verificação, simulações (interrupção paralela, completa) e exercícios abrangentes. As organizações realizam testes com base nos requisitos de continuidade em planos de contingência e incluem uma determinação dos efeitos nas operações, ativos e indivíduos da organização decorrentes de operações de contingência. As organizações têm flexibilidade e discrição na amplitude, profundidade e cronograma das ações corretivas.  
  
**Melhorias do Controle:**

### CP-4(1): Teste do Plano de Contingência | Coordenar com Planos Relacionados

A organização coordena o teste do plano de contingência com os elementos organizacionais responsáveis pelos planos relacionados.  
Guia Adicional: Os planos relacionados aos planos de contingência para sistemas de informações organizacionais incluem, por exemplo, Planos de Continuidade de Negócios, Planos de Recuperação de Desastres, Planos de Continuidade de Operações, Planos de Comunicação de Crises, Planos de Infraestrutura Crítica, Planos de Resposta a Incidentes Cibernéticos e Planos de Emergência de Ocupantes. Esse aprimoramento de controle não exige que as organizações criem elementos organizacionais para lidar com planos relacionados ou que alinhem esses elementos com planos específicos. Requer, no entanto, que se esses elementos organizacionais são responsáveis por planos relacionados, as organizações devem se coordenar com esses elementos.

### CP-4(2): Teste do Plano de Contingência | Local de Processamento Alternativo

A organização testa o plano de contingência no local de processamento alternativo:  
  
a. Familiarizar o pessoal de contingência com a instalação e os recursos disponíveis; e  
  
b. Avaliar os recursos do local de processamento alternativo para suportar operações de contingência.

### CP-4(3): Teste do Plano de Contingência | Testes Automatizados

A organização emprega mecanismos automatizados para testar de maneira mais completa e eficaz o plano de contingência.  
Guia Adicional: Mecanismos automatizados fornecem testes mais completos e eficazes dos planos de contingência, por exemplo: (i) fornecendo uma cobertura mais completa dos problemas de contingência; (ii) selecionando cenários e ambientes de teste mais realistas; e (iii) enfatizando efetivamente o sistema de informação e as missões apoiadas.

### CP-4(4): Teste do Plano de Contingência | Recuperação / Reconstituição Completa

A organização inclui uma recuperação e reconstituição completas do sistema de informações em um estado conhecido como parte dos testes do plano de contingência.

**Referências:**

|  |  |
| --- | --- |
| Diretiva de Continuidade Federal 1 | https://www.fema.gov/media-library-data/1486472423990-f640b42b9073d78693795bb7da4a7af2/January2017FCD1.pdf |
| Publicações de Normas Federais de Processamento de Informações N.199 | http://csrc.nist.gov/publications/PubsFIPS.html#199 |
| Publicação Especial NIST 800-34 | https://csrc.nist.gov/publications/search?keywords-lg=800-34 |
| Publicação Especial NIST 800-84 | https://csrc.nist.gov/publications/search?keywords-lg=800-84 |

## CP-5: Atualização do Plano de Contingência (P0)

**Descrição do Controle:**[Retirado: Incorporado ao CP-2].

## CP-6: Local de Armazenamento Alternativo (P1)

**Descrição do Controle:**A organização:  
  
a. Estabelece um site de armazenamento alternativo, incluindo acordos necessários para permitir o armazenamento e a recuperação de informações de backup do sistema de informações; e  
  
b. Garante que o site de armazenamento alternativo forneça garantias de segurança de informações equivalentes àquelas do site primário.  
  
**Guia Adicional:**Sites de armazenamento alternativo são sites que são geograficamente distintos dos locais de armazenamento primário. Um site de armazenamento alternativo mantém cópias duplicadas de informações e dados, caso o site de armazenamento primário não esteja disponível. Os itens cobertos por contratos de estaleiro alternativo incluem, por exemplo, condições ambientais em locais alternativos, regras de acesso, requisitos de proteção física e ambiental e coordenação da entrega / recuperação de mídia de backup. Os locais alternativos de armazenamento refletem os requisitos dos planos de contingência para que as organizações possam manter as funções essenciais de missão / negócios, apesar da interrupção, comprometimento ou falha nos sistemas de informações organizacionais.  
  
**Melhorias do Controle:**

### CP-6(1): Local de Armazenamento Alternativo | Separação do Local Primário

A organização identifica um local de armazenamento alternativo separado do local de armazenamento primário para reduzir a suscetibilidade às mesmas ameaças.  
Guia Adicional: As ameaças que afetam sites de armazenamento alternativos são geralmente definidas nas avaliações organizacionais de risco e incluem, por exemplo, desastres naturais, falhas estruturais, ataques cibernéticos hostis e erros de omissão / comissão. As organizações determinam o que é considerado um grau suficiente de separação entre sites de armazenamento primário e alternativo, com base nos tipos de ameaças que são preocupantes. Para um tipo específico de ameaça (ou seja, ataques cibernéticos hostis), o grau de separação entre sites é menos relevante.

### CP-6(2): Local de Armazenamento Alternativo | Objetivos De Tempo / Recuperação

A organização configura o local de armazenamento alternativo para facilitar as operações de recuperação de acordo com o tempo de recuperação e os objetivos do ponto de recuperação.

### CP-6(3): Local de Armazenamento Alternativo | Acessibilidade

A organização identifica possíveis problemas de acessibilidade ao local de armazenamento alternativo no caso de uma interrupção ou desastre em toda a área e descreve ações explícitas de mitigação.  
Guia Adicional: As interrupções em toda a área referem-se aos tipos de interrupções de abrangência geográfica (por exemplo, furacão, falta de energia regional) com essas determinações feitas pelas organizações com base em avaliações organizacionais de risco. As ações explícitas de mitigação incluem, por exemplo: (i) duplicação de informações de backup em outros sites de armazenamento alternativos, se ocorrerem problemas de acesso nos sites alternativos originalmente designados; ou (ii) planejar o acesso físico para recuperar as informações de backup se a acessibilidade eletrônica ao site alternativo for interrompida.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-34 | https://csrc.nist.gov/publications/search?keywords-lg=800-34 |

## CP-7: Local de Processamento Alternativo (P1)

**Descrição do Controle:**A organização:  
  
a. Estabelece um site de processamento alternativo incluindo acordos necessários para permitir a transferência e retomada de [Atribuição: operações do sistema de informações definidas pela organização] para missões / funções essenciais dentro de [Atribuição: período de tempo definido pela organização consistente com o tempo de recuperação e objetivos do ponto de recuperação] os principais recursos de processamento não estão disponíveis;  
  
b. Assegura que os equipamentos e suprimentos necessários para transferir e retomar as operações estejam disponíveis no site de processamento alternativo ou que os contratos estejam em vigor para dar suporte à entrega no site dentro do período de tempo definido pela organização para transferência / retomada; e  
  
c. Garante que o site de processamento alternativo forneça garantias de segurança de informações equivalentes às do site primário.  
  
**Guia Adicional:**Sites de processamento alternativos são sites geograficamente distintos dos sites de processamento primários. Um site de processamento alternativo fornece capacidade de processamento no caso de o site de processamento primário não estar disponível. Os itens cobertos por contratos de local de processamento alternativo incluem, por exemplo, condições ambientais em locais alternativos, regras de acesso, requisitos de proteção física e ambiental e coordenação para a transferência / atribuição de pessoal. Os requisitos são especificamente alocados a sites de processamento alternativo que refletem os requisitos dos planos de contingência para manter as funções essenciais de missão / negócios, apesar da interrupção, comprometimento ou falha nos sistemas de informações organizacionais.  
  
**Melhorias do Controle:**

### CP-7(1): Local de Processamento Alternativo | Separação do Local Primário

A organização identifica um local de processamento alternativo separado do local de processamento primário para reduzir a suscetibilidade às mesmas ameaças.  
Guia Adicional: Ameaças que afetam locais de processamento alternativos geralmente são definidas nas avaliações organizacionais de risco e incluem, por exemplo, desastres naturais, falhas estruturais, ataques cibernéticos hostis e erros de omissão / comissão. As organizações determinam o que é considerado um grau suficiente de separação entre sites de processamento primário e alternativo, com base nos tipos de ameaças que são preocupantes. Para um tipo específico de ameaça (ou seja, ataques cibernéticos hostis), o grau de separação entre sites é menos relevante.

### CP-7(2): Local de Processamento Alternativo | Acessibilidade

A organização identifica possíveis problemas de acessibilidade ao local de processamento alternativo no caso de uma interrupção ou desastre em toda a área e descreve ações explícitas de mitigação.  
Guia Adicional: As interrupções em toda a área referem-se aos tipos de interrupções de abrangência geográfica (por exemplo, furacão, falta de energia regional) com essas determinações feitas pelas organizações com base em avaliações organizacionais de risco.

### CP-7(3): Local de Processamento Alternativo | Prioridade do Serviço

A organização desenvolve contratos alternativos de local de processamento que contêm disposições de prioridade de serviço de acordo com os requisitos de disponibilidade organizacional (incluindo objetivos de tempo de recuperação).  
Guia Adicional: Os acordos de prioridade de serviço referem-se a acordos negociados com prestadores de serviços que garantem que as organizações recebam tratamento prioritário consistente com seus requisitos de disponibilidade e a disponibilidade de recursos de informação no site de processamento alternativo.

### CP-7(4): Local de Processamento Alternativo | Preparação para o Uso

A organização prepara o local de processamento alternativo para que ele esteja pronto para ser usado como o site operacional que suporta missões essenciais e funções de negócios.  
Guia Adicional: A preparação do local inclui, por exemplo, o estabelecimento de definições de configuração para os componentes do sistema de informações no local de processamento alternativo, consistente com os requisitos para essas configurações no local primário e a garantia de que suprimentos essenciais e outras considerações logísticas estejam em vigor.

### CP-7(5): Local de Processamento Alternativo | Salvaguardas de Segurança de Informação Equivalentes

[Retirado: Incorporado ao CP-7].

### CP-7(6): Local de Processamento Alternativo | Incapacidade de Voltar ao Local Primário

A organização planeja e se prepara para as circunstâncias que impedem o retorno ao local de processamento primário.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-34 | https://csrc.nist.gov/publications/search?keywords-lg=800-34 |

## CP-8: Serviços de Telecomunicações (P1)

**Descrição do Controle:**A organização estabelece serviços de telecomunicações alternativos, incluindo acordos necessários para permitir a retomada de [Atribuição: operações do sistema de informações definidas pela organização] para missões essenciais e funções comerciais dentro de [Atribuição: período de tempo definido pela organização] quando os recursos primários de telecomunicações não estiverem disponíveis no sites de processamento ou armazenamento primário ou alternativo.  
  
**Guia Adicional:**Esse controle se aplica a serviços de telecomunicações (dados e voz) para sites de processamento e armazenamento primários e alternativos. Os serviços de telecomunicações alternativos refletem os requisitos de continuidade nos planos de contingência para manter missões essenciais / funções de negócios, apesar da perda dos serviços primários de telecomunicações. As organizações podem especificar diferentes períodos de tempo para sites principais / alternativos. Os serviços de telecomunicações alternativos incluem, por exemplo, circuitos / linhas terrestres ou comerciais organizacionais ou comerciais adicionais, em vez de comunicações terrestres. As organizações consideram fatores como disponibilidade, qualidade de serviço e acesso ao celebrar contratos alternativos de telecomunicações.  
  
**Melhorias do Controle:**

### CP-8(1): Serviços de Telecomunicações | Disposições Prioritárias de Serviço

A organização:  
  
a. Desenvolve contratos de serviços de telecomunicações primários e alternativos que contêm provisões de prioridade de serviço de acordo com os requisitos de disponibilidade organizacional (incluindo objetivos de tempo de recuperação); e  
  
b. Solicita prioridade ao serviço de telecomunicações para todos os serviços de telecomunicações usados para preparação para emergências de segurança nacional, caso os serviços de telecomunicações primários e/ou alternativos sejam fornecidos por uma operadora comum.  
Guia Adicional: As organizações consideram o potencial impacto da missão / negócios em situações em que os provedores de serviços de telecomunicações estão atendendo outras organizações com disposições semelhantes de prioridade de serviço.

### CP-8(2): Serviços de Telecomunicações | Pontos Únicos de Falha

A organização obtém serviços alternativos de telecomunicações para reduzir a probabilidade de compartilhar um único ponto de falha com os principais serviços de telecomunicações.

### CP-8(3): Serviços de Telecomunicações | Separação de Prestadores Primários / Alternativos

A organização obtém serviços alternativos de telecomunicações de provedores separados dos provedores de serviços primários para reduzir a suscetibilidade às mesmas ameaças.  
Guia Adicional: As ameaças que afetam os serviços de telecomunicações são tipicamente definidas nas avaliações organizacionais de risco e incluem, por exemplo, desastres naturais, falhas estruturais, ataques cibernéticos / físicos hostis e erros de omissão / comissão. As organizações buscam reduzir suscetibilidades comuns, por exemplo, minimizando a infraestrutura compartilhada entre os provedores de serviços de telecomunicações e alcançando separação geográfica suficiente entre os serviços. As organizações podem considerar o uso de um único provedor de serviços em situações em que o provedor de serviços possa fornecer serviços alternativos de telecomunicações que atendam às necessidades de separação abordadas na avaliação de riscos.

### CP-8(4): Serviços de Telecomunicações | Plano de Contingência de Fornecedores

A organização:  
  
a. Requer que os provedores de serviços de telecomunicações primários e alternativos tenham planos de contingência;  
  
b. Revisa os planos de contingência do provedor para garantir que os planos atendam aos requisitos de contingência organizacional; e  
  
c. Obtém evidência de teste / treinamento de contingência por parte dos fornecedores [Tarefa: frequência definida pela organização].  
Guia Adicional: As revisões dos planos de contingência do fornecedor consideram a natureza proprietária desses planos. Em algumas situações, um resumo dos planos de contingência do fornecedor pode ser evidência suficiente para as organizações atenderem aos requisitos de revisão. Os provedores de serviços de telecomunicações também podem participar de exercícios contínuos de recuperação de desastres em coordenação com o Departamento de Segurança Interna, governos estaduais e locais. As organizações podem usar esses tipos de atividades para satisfazer os requisitos probatórios relacionados às análises, testes e treinamento do plano de contingência do provedor de serviços.

### CP-8(5): Serviços de Telecomunicações | Teste Alternativo do Serviço de Telecomunicações

A organização testa serviços alternativos de telecomunicações [Atribuição: frequência definida pela organização].

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-34 | https://csrc.nist.gov/publications/search?keywords-lg=800-34 |
| DHS: Departamento de Segurança Nacional dos Estados Unidos | http://www.dhs.gov/telecommunications-service-priority-tsp |

## CP-9: Backup do Sistema (P1)

**Descrição do Controle:**A organização:  
  
a. Realiza backups de informações no nível do usuário contidas no sistema de informações [Atribuição: frequência definida pela organização consistente com o tempo de recuperação e objetivos do ponto de recuperação];  
  
b. Realiza backups de informações no nível do sistema contidas no sistema de informações [Atribuição: frequência definida pela organização consistente com o tempo de recuperação e os objetivos do ponto de recuperação];  
  
c. Realiza backups da documentação do sistema de informações, incluindo a documentação relacionada à segurança [Atribuição: frequência definida pela organização, consistente com o tempo de recuperação e os objetivos do ponto de recuperação]; e  
  
d. Protege a confidencialidade, integridade e disponibilidade das informações de backup nos locais de armazenamento.  
  
**Guia Adicional:**As informações no nível do sistema incluem, por exemplo, informações sobre o estado do sistema, sistema operacional e software de aplicativo e licenças. As informações no nível do usuário incluem qualquer informação que não seja a nível do sistema. Os mecanismos empregados pelas organizações para proteger a integridade dos backups de sistemas de informações incluem, por exemplo, assinaturas digitais e hashes criptográficos. A proteção das informações de backup do sistema enquanto em trânsito está além do escopo deste controle. Os backups do sistema de informações refletem os requisitos em planos de contingência, bem como outros requisitos organizacionais para o backup de informações.  
  
**Melhorias do Controle:**

### CP-9(1): Backup do Sistema | Teste de Confiabilidade/Integridade

A organização testa informações de backup [Atribuição: frequência definida pela organização] para verificar a confiabilidade da mídia e a integridade das informações.

### CP-9(2): Backup do Sistema | Restauração de Teste Usando Amostragem

A organização usa uma amostra de informações de backup na restauração de funções selecionadas do sistema de informações como parte dos testes do plano de contingência.

### CP-9(3): Backup do Sistema | Armazenamento Separado para Informação Crítica

A organização armazena cópias de backup de [Atribuição: software do sistema de informações críticas definidas pela organização e outras informações relacionadas à segurança] em uma instalação separada ou em um contêiner classificado para incêndios que não é colocado no sistema operacional.  
Guia Adicional: O software de sistema de informações críticas inclui, por exemplo, sistemas operacionais, sistemas de gerenciamento de chaves criptográficas e sistemas de detecção / prevenção de intrusões. As informações relacionadas à segurança incluem, por exemplo, inventários organizacionais de componentes de hardware, software e firmware. Sites de armazenamento alternativos normalmente servem como instalações de armazenamento separadas para organizações.

### CP-9(4): Backup do Sistema | Proteção Contra Modificação Não Autorizada

[Retirado: Incorporado ao CP-9].

### CP-9(5): Backup do Sistema | Transferir para o Local de Armazenamento Alternativo

A organização transfere as informações de backup do sistema de informações para o local de armazenamento alternativo [Atribuição: período de tempo definido pela organização e taxa de transferência consistente com o tempo de recuperação e os objetivos do ponto de recuperação].  
Guia Adicional: As informações de backup do sistema de informações podem ser transferidas para locais de armazenamento alternativos, eletronicamente ou por remessa física da mídia de armazenamento.

### CP-9(6): Backup do Sistema | Sistema Secundário Redundante

A organização realiza backup do sistema de informações mantendo um sistema secundário redundante que não é colocado no sistema primário e que pode ser ativado sem perda de informações ou interrupção das operações.

### CP-9(7): Backup do Sistema | Autorização Dupla

A organização impõe autorização dupla para a exclusão ou destruição de [Atribuição: informações de backup definidas pela organização].  
Guia Adicional: A autorização dupla garante que a exclusão ou destruição das informações de backup não ocorra a menos que dois indivíduos qualificados realizem a tarefa. Os indivíduos que excluem / destroem informações de backup possuem habilidades / conhecimentos suficientes para determinar se a exclusão / destruição proposta de informações de backup reflete políticas e procedimentos organizacionais. A autorização dupla também pode ser conhecida como controle de duas pessoas.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-34 | https://csrc.nist.gov/publications/search?keywords-lg=800-34 |

## CP-10: Recuperação e Reconstituição do Sistema (P1)

**Descrição do Controle:**A organização fornece a recuperação e reconstituição do sistema de informações para um estado conhecido após uma interrupção, comprometimento ou falha.  
  
**Guia Adicional:**A recuperação está executando atividades do plano de contingência do sistema de informações para restaurar missões organizacionais / funções de negócios. A reconstituição ocorre após a recuperação e inclui atividades para retornar os sistemas de informações organizacionais a estados totalmente operacionais. As operações de recuperação e reconstituição refletem as prioridades da missão e dos negócios, o ponto / hora da recuperação e os objetivos de reconstituição e métricas organizacionais estabelecidas consistentes com os requisitos do plano de contingência. A reconstituição inclui a desativação de quaisquer recursos intermediários do sistema de informações que possam ter sido necessários durante as operações de recuperação. A reconstituição também inclui avaliações de recursos do sistema de informações totalmente restaurados, restabelecimento de atividades de monitoramento contínuo, reautorizações do sistema de informações em potencial e atividades para preparar os sistemas contra interrupções, comprometimentos ou falhas futuras. Os recursos de recuperação / reconstituição empregados pelas organizações podem incluir mecanismos automatizados e procedimentos manuais.  
  
**Melhorias do Controle:**

### CP-10(1): Recuperação e Reconstituição do Sistema | Teste do Plano de Contingência

[Retirado: Incorporado ao CP-4].

### CP-10(2): Recuperação e Reconstituição do Sistema | Recuperação da Transação

O sistema de informações implementa a recuperação de transações para sistemas baseados em transações.  
Guia Adicional: Os sistemas de informação baseados em transações incluem, por exemplo, sistemas de gerenciamento de banco de dados e sistemas de processamento de transações. Os mecanismos que suportam a recuperação de transações incluem, por exemplo, reversão de transações e registro no diário de transações.

### CP-10(3): Recuperação e Reconstituição do Sistema | Controles de Segurança Compensadores

[Retirado: endereçado através de procedimentos de costura].

### CP-10(4): Recuperação e Reconstituição do Sistema | Restaurar Dentro do Período de Tempo

A organização fornece a capacidade de restaurar os componentes do sistema de informações dentro de [Atribuição: períodos de tempo de restauração definidos pela organização] a partir de informações controladas pela configuração e protegidas pela integridade, representando um estado operacional conhecido para os componentes.  
Guia Adicional: A restauração de componentes do sistema de informações inclui, por exemplo, criação de imagens que restaura componentes para estados operacionais conhecidos.

### CP-10(5): Recuperação e Reconstituição do Sistema | Falha na Capacidade

[Retirado: Incorporado no SI-13].

### CP-10(6): Recuperação e Reconstituição do Sistema | Proteção de Componentes

A organização protege hardware, firmware e software de backup e restauração.  
Guia Adicional: A proteção dos componentes de hardware, firmware e software de backup e restauração inclui salvaguardas físicas e técnicas. O software de backup e restauração inclui, por exemplo, tabelas de roteadores, compiladores e outros softwares de sistema relevantes para a segurança.

**Referências:**

|  |  |
| --- | --- |
| Diretiva de Continuidade Federal 1 | https://www.fema.gov/media-library-data/1486472423990-f640b42b9073d78693795bb7da4a7af2/January2017FCD1.pdf |
| Publicação Especial NIST 800-34 | https://csrc.nist.gov/publications/search?keywords-lg=800-34 |

## CP-11: Protocolos de Comunicação Alternativa (P0)

**Descrição do Controle:**O sistema de informações oferece a capacidade de empregar [Atribuição: protocolos de comunicação alternativos definidos pela organização] para apoiar a manutenção da continuidade das operações.  
  
**Guia Adicional:**Os planos de contingência e o treinamento e teste associados a esses planos incorporam um recurso de protocolo de comunicação alternativo como parte do aumento da resiliência dos sistemas de informações organizacionais. Os protocolos de comunicação alternativos incluem, por exemplo, a alternância da versão 4 do TCP / IP (Transmission Control Protocol / Internet Protocol) para a versão 6 do TCP / IP. A troca de protocolos de comunicação pode afetar os aplicativos de software e, portanto, os possíveis efeitos colaterais da introdução de protocolos de comunicação alternativos são: analisados antes da implementação.

## CP-12: Modo de Segurança (P0)

**Descrição do Controle:**O sistema de informações, quando [Atribuição: condições definidas pela organização] for detectado, entra em um modo de operação seguro com [Atribuição: restrições definidas pela organização de modo de operação seguro].  
  
**Guia Adicional:**Para sistemas de informação que suportam missões críticas / funções empresariais incluindo, por exemplo, operações militares e sistemas de armas, operações espaciais civis, operações de usinas nucleares e operações de controle de tráfego aéreo (especialmente ambientes operacionais em tempo real), as organizações podem escolher identificar certas condições sob o qual esses sistemas retornam a um modo de operação seguro predefinido. O modo de operação seguro, que pode ser ativado automaticamente ou manualmente, restringe os tipos de atividades ou operações que os sistemas de informações podem executar quando essas condições são encontradas. A restrição inclui, por exemplo, permitir apenas determinadas funções que poderiam ser realizadas sob potência limitada ou com largura de banda de comunicações reduzida.

## CP-13: Mecanismos de Segurança Alternativos (P0)

**Descrição do Controle:**A organização emprega [Atribuição: mecanismos de segurança alternativos ou suplementares definidos pela organização] para satisfazer [Atribuição: funções de segurança definidas pela organização] quando o principal meio de implementar a função de segurança está indisponível ou comprometido.  
  
**Guia Adicional:**Esse controle suporta a resiliência do sistema de informações e o planejamento / continuidade das operações. Para garantir a continuidade da missão / negócios, as organizações podem implementar mecanismos de segurança alternativos ou suplementares. Esses mecanismos podem ser menos eficazes que os mecanismos primários (por exemplo, não são tão fáceis de usar, nem escalonáveis ou seguros). No entanto, a capacidade de empregar prontamente esses mecanismos alternativos / suplementares aprimora a continuidade geral da missão / negócios que, de outra forma, poderiam ter um impacto adverso se as operações organizacionais precisassem ser reduzidas até que os principais meios de implementação das funções fossem restaurados. Dado o custo e o nível de esforço necessários para fornecer esses recursos alternativos, esse controle normalmente seria aplicado apenas aos recursos críticos de segurança fornecidos por sistemas de informação, componentes de sistema ou serviços de sistema de informação. Por exemplo, uma organização pode emitir para executivos seniores e administradores de sistema almofadas de uso único caso os tokens multifatoriais, o meio padrão da organização para autenticação remota segura, sejam comprometidos.

# IA - Identificação e Autenticação

## IA-1: Política e Procedimentos de Identificação e Autenticação (P1)

**Descrição do Controle:**A organização:  
  
a. Desenvolve, documenta e divulga para [Atribuição: pessoal ou funções definidas pela organização]:  
  
1. Uma política de identificação e autenticação que atenda a finalidade, escopo, funções, responsabilidades, compromisso de gerenciamento, coordenação entre entidades organizacionais e conformidade; e  
  
2. Procedimentos para facilitar a implementação da política de identificação e autenticação e controles associados de identificação e autenticação; e  
  
b. Analisa e atualiza a atual:  
  
1. Política de identificação e autenticação [Atribuição: frequência definida pela organização]; e  
  
2. Procedimentos de identificação e autenticação [Atribuição: frequência definida pela organização].  
  
**Guia Adicional:**Esse controle aborda o estabelecimento de políticas e procedimentos para a implementação efetiva de controles de segurança selecionados e aprimoramentos de controle na família de IA. As políticas e procedimentos refletem as leis federais aplicáveis, ordens executivas, diretivas, regulamentos, políticas, normas e diretrizes. Políticas e procedimentos do programa de segurança no nível da organização podem tornar desnecessária a necessidade de políticas e procedimentos específicos do sistema. A política pode ser incluída como parte da política geral de segurança da informação para organizações ou, inversamente, pode ser representada por múltiplas políticas refletindo a natureza complexa de certas organizações. Os procedimentos podem ser estabelecidos para o programa de segurança em geral e para sistemas de informação específicos, se necessário. A estratégia de gerenciamento de risco organizacional é um fator chave no estabelecimento de políticas e procedimentos.

**Referências:**

|  |  |
| --- | --- |
| Publicações de Normas Federais de Processamento de Informações N.201 | http://csrc.nist.gov/publications/PubsFIPS.html#201 |
| Publicação Especial NIST 800-12 | https://csrc.nist.gov/publications/search?keywords-lg=800-12 |
| Publicação Especial NIST 800-63 | https://csrc.nist.gov/publications/search?keywords-lg=800-63 |
| Publicação Especial NIST 800-73 | https://csrc.nist.gov/publications/search?keywords-lg=800-73 |
| Publicação Especial NIST 800-76 | https://csrc.nist.gov/publications/search?keywords-lg=800-76 |
| Publicação Especial NIST 800-78 | https://csrc.nist.gov/publications/search?keywords-lg=800-78 |
| Publicação Especial NIST 800-100 | https://csrc.nist.gov/publications/search?keywords-lg=800-100 |

## IA-2: Identificação e Autenticação (Usuários Organizacionais) (P1)

**Descrição do Controle:**O sistema de informações identifica e autentica de maneira exclusiva os usuários organizacionais (ou processos agindo em nome dos usuários organizacionais).  
  
**Guia Adicional:**Os usuários organizacionais incluem funcionários ou indivíduos que as organizações consideram ter status equivalente de funcionários (por exemplo, contratados, pesquisadores convidados). Este controle se aplica a todos os acessos que não sejam: (i) acessos explicitamente identificados e documentados no AC-14; e (ii) acessos que ocorrem através do uso autorizado de autenticadores de grupo sem autenticação individual. As organizações podem exigir identificação exclusiva de indivíduos em contas de grupo (por exemplo, contas de privilégios compartilhados) ou para prestação de contas detalhada de atividades individuais. As organizações empregam senhas, tokens ou biometria para autenticar identidades de usuários ou, no caso, autenticação multifatorial ou alguma combinação delas. O acesso aos sistemas de informações organizacionais é definido como acesso local ou acesso à rede. Acesso local é qualquer acesso aos sistemas de informações organizacionais por usuários (ou processos agindo em nome dos usuários), onde esse acesso é obtido por conexões diretas sem o uso de redes. Acesso à rede é o acesso aos sistemas de informações organizacionais pelos usuários (ou processos agindo em nome dos usuários), onde esse acesso é obtido por meio de conexões de rede (ou seja, acessos não locais). O acesso remoto é um tipo de acesso à rede que envolve comunicação através de redes externas (por exemplo, a Internet). Redes internas incluem redes de área local e redes de área ampla. Além disso, o uso de redes privadas virtuais criptografadas (VPNs) para conexões de rede entre endpoints controlados pela organização e endpoints não controlados pela organização pode ser tratado como redes internas a partir da perspectiva de proteger a confidencialidade e integridade das informações que atravessam a rede. As organizações podem satisfazer os requisitos de identificação e autenticação nesse controle, cumprindo os requisitos da Diretiva Presidencial de Segurança Interna 12, consistentes com os planos de implementação organizacional específicos. A autenticação multifator exige o uso de dois ou mais fatores diferentes para obter a autenticação. Os fatores são definidos como: (i) algo que você conhece (por exemplo, senha, número de identificação pessoal [PIN]); (ii) algo que você possui (por exemplo, dispositivo de identificação criptográfica, token); ou (iii) algo que você é (por exemplo, biométrico). As soluções que possuem múltiplo fator que exigem dispositivos separados dos sistemas de informação que obtêm acesso incluem, por exemplo, tokens de hardware que fornecem autenticadores baseados em tempo ou resposta a contestação e cartões inteligentes, como o cartão de verificação de identidade pessoal do governo dos EUA e o cartão de acesso comum DoD. Além de identificar e autenticar usuários no nível do sistema de informações (ou seja, no login), as organizações também empregam mecanismos de identificação e autenticação no nível do aplicativo, quando necessário, para fornecer maior segurança das informações. Os requisitos de identificação e autenticação para outros usuários que não sejam organizacionais estão descritos no IA-8.  
  
**Melhorias do Controle:**

### IA-2(1): Identificação e Autenticação (Usuários Organizacionais) | Identificação e Autenticação (Usuários Organizacionais) | Acesso à Rede para Contas Privilegiadas

O sistema de informações implementa a autenticação multifator para acesso da rede a contas privilegiadas.

### IA-2(2): Identificação e Autenticação (Usuários Organizacionais) | Identificação e Autenticação (Usuários Organizacionais) | Acesso à Rede para Contas Não Privilegiadas

O sistema de informações implementa a autenticação multifator para acesso à rede de contas não privilegiadas.

### IA-2(3): Identificação e Autenticação (Usuários Organizacionais) | Identificação e Autenticação (Usuários Organizacionais) | Acesso Local a Contas Privilegiadas

O sistema de informações implementa autenticação multifator para acesso local a contas privilegiadas.

### IA-2(4): Identificação e Autenticação (Usuários Organizacionais) | Identificação e Autenticação (Usuários Organizacionais) | Acesso Local a Contas Não Privilegiadas

O sistema de informações implementa a autenticação multifator para acesso local a contas não privilegiadas.

### IA-2(5): Identificação e Autenticação (Usuários Organizacionais) | Identificação e Autenticação (Usuários Organizacionais) | Autenticação de Grupo

A organização exige que os indivíduos sejam autenticados com um autenticador individual quando um autenticador de grupo é empregado.  
Guia Adicional: Exigir que os indivíduos usem autenticadores individuais como um segundo nível de autenticação ajuda as organizações a reduzir o risco de usar autenticadores de grupo.

### IA-2(6): Identificação e Autenticação (Usuários Organizacionais) | Identificação e Autenticação (Usuários Organizacionais) | Acesso à Rede de Contas Privilegiadas - Dispositivo Separado

O sistema de informações implementa a autenticação multifatorial para o acesso da rede a contas privilegiadas, de modo que um dos fatores seja fornecido por um dispositivo separado do sistema que obtém acesso e o dispositivo atenda [Atribuição: requisitos de força definidos pelos mecanismos da organização].

### IA-2(7): Identificação e Autenticação (Usuários Organizacionais) | Identificação e Autenticação (Usuários Organizacionais) | Acesso à Rede de Contas Não Privilegiadas - Dispositivo Separado

O sistema de informações implementa autenticação multifatorial para acesso de rede a contas não privilegiadas, de modo que um dos fatores seja fornecido por um dispositivo separado do sistema que obtém acesso e o dispositivo atenda [Atribuição: requisitos de força definidos pelo mecanismo da organização].

### IA-2(8): Identificação e Autenticação (Usuários Organizacionais) | Identificação e Autenticação (Usuários Organizacionais) | Acesso à Rede de Contas Privilegiadas - Resistente contra Replay

O sistema de informações implementa mecanismos de autenticação resistentes a repetições para acesso da rede a contas privilegiadas.  
Guia Adicional: Os processos de autenticação resistem a ataques de repetição, se for impraticável obter autenticações bem-sucedidas, reproduzindo mensagens de autenticação anteriores. As técnicas resistentes à reprodução incluem, por exemplo, protocolos que usam nonces ou desafios, como Transport Layer Security (TLS) e autenticadores de tempo síncrono ou resposta a desafio.

### IA-2(9): Identificação e Autenticação (Usuários Organizacionais) | Identificação e Autenticação (Usuários Organizacionais) | Acesso à Rede de Contas Não Privilegiadas - Resistente contra Replay

O sistema de informações implementa mecanismos de autenticação resistentes a repetições para acesso da rede a contas não privilegiadas.  
Guia Adicional: Os processos de autenticação resistem a ataques de repetição, se for impraticável obter autenticações bem-sucedidas gravando / reproduzindo mensagens de autenticação anteriores. As técnicas resistentes à reprodução incluem, por exemplo, protocolos que usam nonces ou desafios, como Transport Layer Security (TLS) e autenticadores de tempo síncrono ou resposta a desafio.

### IA-2(10): Identificação e Autenticação (Usuários Organizacionais) | Identificação e Autenticação (Usuários Organizacionais) | Single Sign-On

O sistema de informações fornece um recurso de login único para [Atribuição: contas e serviços do sistema de informações definido pela organização].  
Guia Adicional: O login único permite que os usuários efetuem login uma vez e obtenham acesso a vários recursos do sistema de informações. As organizações consideram as eficiências operacionais fornecidas pelos recursos de login único com o risco aumentado das divulgações de autenticadores únicos que fornecem acesso a vários recursos do sistema.

### IA-2(11): Identificação e Autenticação (Usuários Organizacionais) | Identificação e Autenticação (Usuários Organizacionais) | Acesso Remoto - Dispositivo Separado

O sistema de informações implementa a autenticação multifatorial para acesso remoto a contas privilegiadas e não privilegiadas, de modo que um dos fatores seja fornecido por um dispositivo separado do sistema que obtém acesso e o dispositivo atenda [Atribuição: requisitos de força definidos pelos mecanismos da organização].  
Guia Adicional: Para acesso remoto a contas privilegiadas / não privilegiadas, o objetivo de exigir que um dispositivo separado do sistema de informações obtenha acesso a um dos fatores durante a autenticação multifator é reduzir a probabilidade de comprometer as credenciais de autenticação armazenadas no sistema. Por exemplo, os adversários que implantam código malicioso nos sistemas de informações organizacionais podem comprometer essas credenciais residentes no sistema e, posteriormente, se passar por usuários autorizados.

### IA-2(12): Identificação e Autenticação (Usuários Organizacionais) | Identificação e Autenticação (Usuários Organizacionais) | Aceitação de Credenciais PIV

O sistema de informações aceita e verifica eletronicamente as credenciais de verificação de identidade pessoal (PIV).  
Guia Adicional: Esse aprimoramento de controle se aplica a organizações que implementam sistemas de controle de acesso lógico (LACS) e sistemas de controle de acesso físico (PACS). As credenciais de verificação de identidade pessoal (PIV) são aquelas emitidas por agências federais que estão em conformidade com a publicação FIPS 201 e com os documentos de orientação. O Memorando OMB 11-11 exige que as agências federais continuem implementando os requisitos especificados no HSPD-12 para permitir o uso de credenciais de PIV em toda a agência.

### IA-2(13): Identificação e Autenticação (Usuários Organizacionais) | Identificação e Autenticação (Usuários Organizacionais) | Autenticação Out-Of-Band

O sistema de informações implementa [Atribuição: autenticação fora de banda definida pela organização] em [Atribuição: condições definidas pela organização].  
Guia Adicional: A autenticação fora da banda (OOBA) refere-se ao uso de dois caminhos de comunicação separados para identificar e autenticar usuários ou dispositivos em um sistema de informações. O primeiro caminho (ou seja, o caminho dentro da banda), é usado para identificar e autenticar usuários ou dispositivos, e geralmente é o caminho pelo qual as informações fluem. O segundo caminho (ou seja, o caminho fora da banda) é usado para verificar independentemente a autenticação e/ou a ação solicitada. Por exemplo, um usuário se autentica através de um notebook em um servidor remoto ao qual deseja acessar e solicita alguma ação do servidor por esse caminho de comunicação. Posteriormente, o servidor entra em contato com o usuário por meio do telefone celular do usuário para verificar se a ação solicitada se originou do usuário. O usuário pode confirmar a ação pretendida para um indivíduo no telefone ou fornecer um código de autenticação via telefone. Esse tipo de autenticação pode ser empregado pelas organizações para atenuar ataques reais ou suspeitos. As condições para ativação podem incluir, por exemplo, atividades suspeitas, novos indicadores de ameaça ou níveis elevados de ameaça ou o nível de impacto ou nível de classificação das informações nas transações solicitadas.

**Referências:**

|  |  |
| --- | --- |
| DHS - HSPD-12 | https://www.dhs.gov/homeland-security-presidential-directive-12 |
| OMB Memorando 04-04 | https://georgewbush-whitehouse.archives.gov/omb/memoranda/fy04/m04-04.pdf |
| OMB Memorando 06-16 | https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2006/m06-16.pdf |
| OMB Memorando 11-11 | https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2011/m11-11.pdf |
| Publicações de Normas Federais de Processamento de Informações N.201 | http://csrc.nist.gov/publications/PubsFIPS.html#201 |
| Publicação Especial NIST 800-63 | https://csrc.nist.gov/publications/search?keywords-lg=800-63 |
| Publicação Especial NIST 800-73 | https://csrc.nist.gov/publications/search?keywords-lg=800-73 |
| Publicação Especial NIST 800-76 | https://csrc.nist.gov/publications/search?keywords-lg=800-76 |
| Publicação Especial NIST 800-78 | https://csrc.nist.gov/publications/search?keywords-lg=800-78 |
| FICAM - Roteiro e Orientação para Implementação | http://www.idmanagement.gov/documents/ficam-roadmap-and-implementation-guidance |
| FICAM: Identidade Federal, Credencial e Gerenciamento de Acesso | http://idmanagement.gov |

## IA-3: Identificação e Autenticação do Dispositivo (P1)

**Descrição do Controle:**O sistema de informações identifica e autentica exclusivamente [Atribuição: tipos e/ou tipos de dispositivos definidos pela organização] antes de estabelecer uma [Seleção (um ou mais): local; controlo remoto; conexão de rede.  
  
**Guia Adicional:**Os dispositivos organizacionais que exigem identificação e autenticação exclusivas de dispositivo a dispositivo podem ser definidos por tipo, por dispositivo ou por uma combinação de tipo / dispositivo. Os sistemas de informação geralmente usam informações conhecidas compartilhadas (por exemplo, endereços de Controle de Acesso à Mídia [MAC] ou TCP / IP) para identificação de dispositivos ou soluções de autenticação organizacional (por exemplo, IEEE 802.1xe Protocolo de Autenticação Extensível [EAP]). ], Servidor Radius com autenticação TLB (EAP-Transport Layer Security), Kerberos) para identificar / autenticar dispositivos em redes locais e/ou de longa distância. As organizações determinam a força necessária dos mecanismos de autenticação pelas categorias de segurança dos sistemas de informação. Devido aos desafios de aplicar esse controle em grande escala, as organizações são encorajadas a aplicar o controle somente a esses números limitados (e tipo) de dispositivos que realmente precisam suportar esse recurso.  
  
**Melhorias do Controle:**

### IA-3(1): Identificação e Autenticação do Dispositivo | Autenticação Bidirecional Criptográfica

O sistema de informação autentica [Atribuição: dispositivos específicos definidos pela organização e/ou tipos de dispositivos] antes de estabelecer [Seleção (um ou mais): local; controlo remoto; rede] usando autenticação bidirecional baseada em criptografia.  
Guia Adicional: Uma conexão local é qualquer conexão com um dispositivo que esteja se comunicando sem o uso de uma rede. Uma conexão de rede é qualquer conexão com um dispositivo que se comunica através de uma rede (por exemplo, rede local ou de área ampla, Internet). Uma conexão remota é qualquer conexão com um dispositivo que se comunica através de uma rede externa (por exemplo, a Internet). A autenticação bidirecional fornece proteções mais fortes para validar a identidade de outros dispositivos para conexões com maior risco (por exemplo, conexões remotas).

### IA-3(2): Identificação e Autenticação do Dispositivo | Autenticação de Rede Bidirecional Criptográfica

[Retirado: Incorporado no IA-3 (1)].

### IA-3(3): Identificação e Autenticação do Dispositivo | Alocação de Endereço Dinâmico

A organização:  
  
a. Padroniza as informações de concessão de alocação dinâmica de endereço e a duração da concessão atribuída aos dispositivos de acordo com [Atribuição: informações de concessão definidas pela organização e duração da concessão]; e  
  
b. As auditorias concedem informações quando atribuídas a um dispositivo.  
Guia Adicional: Clientes habilitados para DHCP, obtendo concessões para endereços IP de servidores DHCP, são um exemplo típico de alocação dinâmica de endereços para dispositivos.

### IA-3(4): Identificação e Autenticação do Dispositivo | Atestação do Dispositivo

A organização garante que a identificação e autenticação do dispositivo com base no atestado sejam tratadas por [Atribuição: processos de gerenciamento de configurações definidas pela organização].  
Guia Adicional: O atestado de dispositivo refere-se à identificação e autenticação de um dispositivo com base em sua configuração e estado operacional conhecido. Isso pode ser determinado através de algum hash criptográfico do dispositivo. Se o atestado do dispositivo é o meio de identificação e autenticação, é importante que as correções e atualizações do dispositivo sejam tratadas por meio de um processo de gerenciamento de configuração, para que essas correções / atualizações sejam feitas com segurança e, ao mesmo tempo, não atrapalhem a identificação e autenticação para outros dispositivos.

## IA-4: Gestão do Identificador (P1)

**Descrição do Controle:**A organização gerencia identificadores de sistema de informações por:  
  
a. Recebendo autorização de [Atribuição: pessoal ou funções definidas pela organização] para atribuir um indivíduo, grupo, função ou identificador de dispositivo;  
  
b. Selecionando um identificador que identifica um indivíduo, grupo, função ou dispositivo;  
  
c. Atribuir o identificador ao indivíduo, grupo, função ou dispositivo pretendido;  
  
d. Impedindo a reutilização de identificadores para [Atribuição: período definido pela organização]; e  
  
e. Desativando o identificador após [Atribuição: período de inatividade definido pela organização].  
  
**Guia Adicional:**Os identificadores comuns de dispositivos incluem, por exemplo, MAC (controle de acesso à mídia), endereços IP (Internet Protocol) ou identificadores de token exclusivos do dispositivo. O gerenciamento de identificadores individuais não é aplicável a contas do sistema de informações compartilhadas (por exemplo, contas de convidado e anônimas). Normalmente, os identificadores individuais são os nomes de usuários das contas do sistema de informações atribuídas a esses indivíduos. Nesses casos, as atividades de gerenciamento de conta do AC-2 usam nomes de conta fornecidos pelo IA-4. Esse controle também aborda identificadores individuais não necessariamente associados às contas do sistema de informações (por exemplo, identificadores usados nos bancos de dados de controle de segurança física acessados pelos sistemas de leitores de crachás para acesso aos sistemas de informações). Impedir a reutilização de identificadores implica impedir a atribuição de identificadores de indivíduos, grupos, funções ou dispositivos usados anteriormente a diferentes indivíduos, grupos, funções ou dispositivos.  
  
**Melhorias do Controle:**

### IA-4(1): Gestão do Identificador | Proibir Identificadores de Conta como Identificadores Públicos

A organização proíbe o uso de identificadores de contas do sistema de informações iguais aos identificadores públicos para contas individuais de correio eletrônico.  
Guia Adicional: Proibir o uso de identificadores de conta de sistemas de informação que sejam iguais a alguns identificadores públicos, como a seção de identificador individual de um endereço de correio eletrônico, torna mais difícil para os adversários adivinharem identificadores de usuários em sistemas de informações organizacionais.

### IA-4(2): Gestão do Identificador | Autorização de Supervisor

A organização exige que o processo de registro para receber um identificador individual inclua autorização do supervisor.

### IA-4(3): Gestão do Identificador | Várias Formas de Certificação

A organização exige que várias formas de certificação de identificação individual sejam apresentadas à autoridade de registro.  
Guia Adicional: A exigência de várias formas de identificação, como evidência documental ou uma combinação de documentos e biometria, reduz a probabilidade de os indivíduos usarem identificação fraudulenta para estabelecer uma identidade ou, pelo menos, aumenta o fator de trabalho de possíveis adversários.

### IA-4(4): Gestão do Identificador | Identificar o Estado do Usuário

A organização gerencia identificadores individuais, identificando exclusivamente cada indivíduo como [Atribuição: característica definida pela organização que identifica o status individual].  
Guia Adicional: As características que identificam o status dos indivíduos incluem, por exemplo, contratados e cidadãos estrangeiros. A identificação do status dos indivíduos por características específicas fornece informações adicionais sobre as pessoas com quem o pessoal da organização está se comunicando. Por exemplo, pode ser útil para um funcionário do governo saber que um dos indivíduos em uma mensagem de e-mail é um contratado.

### IA-4(5): Gestão do Identificador | Gestão Dinâmica

O sistema de informações gerencia dinamicamente identificadores.  
Guia Adicional: Em contraste com as abordagens convencionais de identificação que presumem contas estáticas para usuários pré-registrados, muitos sistemas de informações distribuídos, incluindo, por exemplo, arquiteturas orientadas a serviços, dependem do estabelecimento de identificadores em tempo de execução para entidades que antes eram desconhecidas. Nessas situações, as organizações antecipam e fornecem o estabelecimento dinâmico de identificadores. Relações de confiança pré-estabelecidas e mecanismos com autoridades apropriadas para validar identidades e credenciais relacionadas são essenciais.

### IA-4(6): Gestão do Identificador | Gestão de Organização Transversal

A organização coordena com [Atribuição: organizações externas definidas pela organização] para gerenciamento de identificadores entre organizações.  
Guia Adicional: O gerenciamento de identificadores entre organizações fornece às organizações a capacidade de identificar adequadamente indivíduos, grupos, funções ou dispositivos ao realizar atividades entre organizações que envolvem o processamento, armazenamento ou transmissão de informações.

### IA-4(7): Gestão do Identificador | Inscrição em Pessoa

A organização exige que o processo de registro para receber um identificador individual seja conduzido pessoalmente perante uma autoridade de registro designada.  
Guia Adicional: O registro pessoal reduz a probabilidade de emissão de identificadores fraudulentos, porque requer a presença física de indivíduos e interações presenciais reais com as autoridades de registro designadas.

**Referências:**

|  |  |
| --- | --- |
| Publicações de Normas Federais de Processamento de Informações N.201 | http://csrc.nist.gov/publications/PubsFIPS.html#201 |
| Publicação Especial NIST 800-73 | https://csrc.nist.gov/publications/search?keywords-lg=800-73 |
| Publicação Especial NIST 800-76 | https://csrc.nist.gov/publications/search?keywords-lg=800-76 |
| Publicação Especial NIST 800-78 | https://csrc.nist.gov/publications/search?keywords-lg=800-78 |

## IA-5: Gestão do Autenticador (P1)

**Descrição do Controle:**A organização gerencia autenticadores de sistemas de informações por:  
  
a. Verificar, como parte da distribuição inicial do autenticador, a identidade do indivíduo, grupo, função ou dispositivo que recebe o autenticador;  
  
b. Estabelecer conteúdo inicial do autenticador para autenticadores definido pela organização;  
  
c. Garantir que os autenticadores tenham força de mecanismo suficiente para o uso pretendido;  
  
d. Estabelecer e implementar procedimentos administrativos para distribuição inicial de autenticadores, para autenticadores perdidos / comprometidos ou danificados e para revogar autenticadores;  
  
e. Alteração do conteúdo padrão dos autenticadores antes da instalação do sistema de informações;  
  
f. Estabelecer restrições de vida útil mínima e máxima e condições de reutilização para autenticadores;  
  
g. Alteração / atualização de autenticadores [Atribuição: período definido pela organização por tipo de autenticador];  
  
h. Proteger o conteúdo do autenticador contra divulgação e modificação não autorizadas;  
  
i. Exigir que os indivíduos tomem e mandem implementar dispositivos, salvaguardas de segurança específicas para proteger os autenticadores; e  
  
j. Alteração de autenticadores para contas de grupo / função quando a associação a essas contas é alterada.  
  
**Guia Adicional:**Os autenticadores individuais incluem, por exemplo, senhas, tokens, biometria, certificados PKI e cartões-chave. O conteúdo inicial do autenticador é o conteúdo real (por exemplo, a senha inicial), em oposição aos requisitos sobre o conteúdo do autenticador (por exemplo, tamanho mínimo da senha). Em muitos casos, os desenvolvedores enviam componentes do sistema de informações com credenciais de autenticação padrão de fábrica para permitir a instalação e configuração inicial. As credenciais de autenticação padrão geralmente são bem conhecidas, facilmente detectáveis e apresentam um risco de segurança significativo. O requisito de proteger autenticadores individuais pode ser implementado via controle PL-4 ou PS-6 para autenticadores em posse de indivíduos e pelos controles AC-3, AC-6 e SC-28 para autenticadores armazenados em sistemas de informações organizacionais (por exemplo, senhas armazenadas em formatos com hash ou criptografados, arquivos contendo senhas criptografadas ou com hash acessíveis com privilégios de administrador). Os sistemas de informação suportam o gerenciamento de autenticadores individuais por configurações e restrições definidas pela organização para várias características do autenticador, incluindo, por exemplo, tamanho mínimo de senha, composição de senhas, janela de tempo de validação para tokens únicos síncronos por tempo e número de rejeições permitidas durante o estágio de verificação autenticação biométrica. As ações específicas que podem ser tomadas para proteger os autenticadores incluem, por exemplo, manter a posse de autenticadores individuais, não emprestar ou compartilhar autenticadores individuais com outras pessoas e relatar autenticadores perdidos, roubados ou comprometidos imediatamente. O gerenciamento do autenticador inclui emitir e revogar, quando não for mais necessário, autenticadores para acesso temporário, como o necessário para manutenção remota. Os autenticadores de dispositivos incluem, por exemplo, certificados e senhas.  
  
**Melhorias do Controle:**

### IA-5(1): Gestão do Autenticador | Autenticação Baseada em Senha

O sistema de informações, para autenticação baseada em senha:  
  
a. Impõe a complexidade mínima da senha de [Atribuição: requisitos definidos pela organização para distinção entre maiúsculas e minúsculas, número de caracteres, combinação de letras maiúsculas, minúsculas, números e caracteres especiais, incluindo requisitos mínimos para cada tipo];  
  
b. Aplica pelo menos o seguinte número de caracteres alterados quando novas senhas são criadas: [Atribuição: número definido pela organização];  
  
c. Armazena e transmite apenas senhas protegidas por criptografia;  
  
d. Força as restrições de vida útil mínima e máxima da senha de [Atribuição: números definidos pela organização para duração mínima, duração máxima];  
  
e. Proíbe a reutilização de senha por gerações [de atribuição: número definido pela organização]; e  
  
f. Permite o uso de uma senha temporária para logins do sistema com uma alteração imediata em uma senha permanente.  
Guia Adicional: Esse aprimoramento de controle se aplica à autenticação de fator único de indivíduos que usam senhas como autenticadores individuais ou de grupo e de maneira semelhante, quando as senhas fazem parte de autenticadores multifatoriais. Esse aprimoramento de controle não se aplica quando as senhas são usadas para desbloquear autenticadores de hardware (por exemplo, cartões de verificação de identidade pessoal). A implementação desses mecanismos de senha pode não atender a todos os requisitos do aprimoramento. As senhas protegidas por criptografia incluem, por exemplo, versões criptografadas de senhas e hashes criptográficos unidirecionais de senhas. O número de caracteres alterados refere-se ao número de alterações necessárias em relação ao número total de posições na senha atual. As restrições de duração da senha não se aplicam a senhas temporárias. Para mitigar certos ataques de força bruta contra senhas, as organizações também podem considerar salgar senhas.

### IA-5(2): Gestão do Autenticador | Autenticação Baseada em PKI

O sistema de informações, para autenticação baseada em PKI:  
  
a. Valida certificações construindo e verificando um caminho de certificação para uma âncora de confiança aceita, incluindo a verificação de informações de status do certificado;  
  
b. Impõe acesso autorizado à chave privada correspondente;  
  
c. Mapeia a identidade autenticada para a conta do indivíduo ou grupo; e  
  
d. Implementa um cache local de dados de revogação para oferecer suporte à descoberta e validação de caminhos em caso de incapacidade de acessar informações de revogação pela rede.  
Guia Adicional: As informações de status dos caminhos de certificação incluem, por exemplo, listas de revogação de certificados ou respostas do protocolo de status de certificados. Para cartões PIV, a validação de certificações envolve a construção e a verificação de um caminho de certificação para a âncora de confiança da Common Policy Root, incluindo o processamento da política de certificado.

### IA-5(3): Gestão do Autenticador | Inscrição Pessoal ou de Terceiro Confiável

A organização exige que o processo de registro para receber [Tarefa: tipos definidos pela organização e/ou autenticadores específicos] seja conduzido [Seleção: pessoalmente; por um terceiro confiável] antes de [Cessão: autoridade de registro definida pela organização] com autorização por [Cessão: pessoal ou função definida pela organização].

### IA-5(4): Gestão do Autenticador | Suporte Automatizado para Determinação da Força de Senha

A organização emprega ferramentas automatizadas para determinar se os autenticadores de senha são suficientemente fortes para satisfazer [Atribuição: requisitos definidos pela organização].  
Guia Adicional: Esse aprimoramento de controle concentra-se na criação de senhas fortes e nas características de tais senhas (por exemplo, complexidade) antes do uso, cuja aplicação é realizada pelos sistemas de informações organizacionais no IA-5 (1).

### IA-5(5): Gestão do Autenticador | Alterar Autenticadores Antes da Entrega

A organização exige que desenvolvedores / instaladores de componentes do sistema de informações forneçam autenticadores exclusivos ou alterem os autenticadores padrão antes da entrega / instalação.  
Guia Adicional: Esse aprimoramento de controle estende o requisito para as organizações alterarem os autenticadores padrão na instalação do sistema de informações, exigindo que os desenvolvedores e/ou instaladores forneçam autenticadores exclusivos ou alterem os autenticadores padrão dos componentes do sistema antes da entrega e/ou instalação. No entanto, normalmente não se aplica aos desenvolvedores de produtos comerciais de tecnologia da informação. Os requisitos para autenticadores exclusivos podem ser incluídos nos documentos de aquisição preparados pelas organizações ao adquirir sistemas de informação ou componentes de sistema.

### IA-5(6): Gestão do Autenticador | Proteção de Autenticadores

A organização protege os autenticadores proporcionais à categoria de segurança das informações às quais o uso do autenticador permite acesso.  
Guia Adicional: Para sistemas de informações que contêm várias categorias de segurança de informações sem separação física ou lógica confiável entre categorias, os autenticadores usados para conceder acesso aos sistemas são protegidos proporcionalmente à categoria de informações de segurança mais alta dos sistemas.

### IA-5(7): Gestão do Autenticador | Autenticadores Estáticos Não Criptografados, Não Embutidos

A organização garante que os autenticadores estáticos não criptografados não sejam incorporados nos aplicativos ou acessem scripts ou armazenados nas teclas de função.  
Guia Adicional: As organizações têm cuidado ao determinar se os autenticadores incorporados ou armazenados estão no formato criptografado ou não criptografado. Se os autenticadores forem usados da maneira armazenada, essas representações serão consideradas autenticadores não criptografados. Isso independentemente da representação ser talvez uma versão criptografada de outra coisa (por exemplo, uma senha).

### IA-5(8): Gestão do Autenticador | Múltiplas Contas do Sistema de Informação

A organização implementa [Atribuição: salvaguardas de segurança definidas pela organização] para gerenciar o risco de comprometimento devido ao fato de as pessoas terem contas em vários sistemas de informação.  
Guia Adicional: Quando indivíduos têm contas em vários sistemas de informações, existe o risco de que o comprometimento de uma conta possa levar ao comprometimento de outras contas, se os indivíduos usarem os mesmos autenticadores. As alternativas possíveis incluem, por exemplo: (i) ter diferentes autenticadores em todos os sistemas; (ii) empregando alguma forma de mecanismo de login único; ou (iii) incluindo alguma forma de senhas únicas em todos os sistemas.

### IA-5(9): Gestão do Autenticador | Gestão das Credenciais de Múltiplas Organizações

A organização coordena com [Atribuição: organizações externas definidas pela organização] para gerenciamento de credenciais entre organizações.  
Guia Adicional: O gerenciamento de credenciais entre organizações fornece a capacidade de as organizações autenticarem adequadamente indivíduos, grupos, funções ou dispositivos ao realizar atividades entre organizações que envolvem o processamento, armazenamento ou transmissão de informações.

### IA-5(10): Gestão do Autenticador | Associação Dinâmica de Credencial

O sistema de informação fornece dinamicamente identidades.  
Guia Adicional: A autenticação requer alguma forma de ligação entre uma identidade e o autenticador usado para confirmar a identidade. Nas abordagens convencionais, essa ligação é estabelecida pré-provisionando a identidade e o autenticador para o sistema de informações. Por exemplo, a ligação entre um nome de usuário (identidade) e uma senha (autenticador) é realizada fornecendo a identidade e o autenticador como um par no sistema de informações. Novas técnicas de autenticação permitem que a ligação entre a identidade e o autenticador seja implementada fora de um sistema de informações. Por exemplo, com credenciais de cartão inteligente, a identidade e o autenticador são vinculados no cartão. Usando essas credenciais, os sistemas de informação podem autenticar identidades que não foram pré-provisionadas, provisionando dinamicamente a identidade após a autenticação. Nessas situações, as organizações podem antecipar o provisionamento dinâmico de identidades. Relações de confiança pré-estabelecidas e mecanismos com autoridades apropriadas para validar identidades e credenciais relacionadas são essenciais.

### IA-5(11): Gestão do Autenticador | Autenticação Baseada em Token de Hardware

O sistema de informações, para autenticação baseada em token de hardware, emprega mecanismos que satisfazem [Atribuição: requisitos de qualidade de token definidos pela organização].  
Guia Adicional: A autenticação baseada em token de hardware normalmente se refere ao uso de tokens baseados em PKI, como o cartão de verificação de identidade pessoal do governo dos EUA (PIV). As organizações definem requisitos específicos para tokens, como trabalhar com uma PKI específica.

### IA-5(12): Gestão do Autenticador | Autenticação Baseada em Biometria

O sistema de informações, para autenticação baseada em biometria, emprega mecanismos que atendem [Atribuição: requisitos de qualidade biométricos definidos pela organização].  
Guia Adicional: Diferentemente da autenticação baseada em senha, que fornece correspondências exatas das senhas de entrada do usuário às senhas armazenadas, a autenticação biométrica não fornece essas correspondências exatas. Dependendo do tipo de biometria e do tipo de mecanismo de coleta, é provável que haja alguma divergência entre a biometria apresentada e a biométrica armazenada, que serve como base de comparação. Provavelmente haverá falsos positivos e falsos negativos ao fazer essas comparações. A taxa na qual as taxas de aceitação falsa e de rejeição falsa são iguais é conhecida como taxa de cruzamento. Os requisitos de qualidade biométrica incluem, por exemplo, taxas de cruzamento aceitáveis, pois isso reflete essencialmente a precisão da biometria.

### IA-5(13): Gestão do Autenticador | Expiração de Autenticadores em Cache

O sistema de informações proíbe o uso de autenticadores em cache após [Atribuição: período definido pela organização].

### IA-5(14): Gestão do Autenticador | Gerenciando o Conteúdo das Lojas de Confiança PKI

A organização, para autenticação baseada em PKI, emprega uma metodologia deliberada em toda a organização para gerenciar o conteúdo dos armazenamentos confiáveis da PKI instalados em todas as plataformas, incluindo redes, sistemas operacionais, navegadores e aplicativos.

### IA-5(15): Gestão do Autenticador | Produtos e Serviços Aprovados pela FICAM

A organização usa apenas produtos e serviços de descoberta e validação de caminho aprovados pela FICAM.  
Guia Adicional: Os produtos e serviços de descoberta e validação de caminho aprovados pela Identidade Federal, Credencial e Gerenciamento de Acesso (FICAM) são aqueles que foram aprovados pelo programa de conformidade da FICAM, quando aplicável.

**Referências:**

|  |  |
| --- | --- |
| OMB Memorando 04-04 | https://georgewbush-whitehouse.archives.gov/omb/memoranda/fy04/m04-04.pdf |
| OMB Memorando 11-11 | https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2011/m11-11.pdf |
| Publicações de Normas Federais de Processamento de Informações N.201 | http://csrc.nist.gov/publications/PubsFIPS.html#201 |
| Publicação Especial NIST 800-63 | https://csrc.nist.gov/publications/search?keywords-lg=800-63 |
| Publicação Especial NIST 800-73 | https://csrc.nist.gov/publications/search?keywords-lg=800-73 |
| Publicação Especial NIST 800-76 | https://csrc.nist.gov/publications/search?keywords-lg=800-76 |
| Publicação Especial NIST 800-78 | https://csrc.nist.gov/publications/search?keywords-lg=800-78 |
| FICAM - Roteiro e Orientação para Implementação | http://www.idmanagement.gov/documents/ficam-roadmap-and-implementation-guidance |
| FICAM: Identidade Federal, Credencial e Gerenciamento de Acesso | http://idmanagement.gov |

## IA-6: Feedback do Autenticador (P2)

**Descrição do Controle:**O sistema de informações oculta o feedback das informações de autenticação durante o processo de autenticação para proteger as informações contra possíveis explorações / usos por indivíduos não autorizados.  
  
**Guia Adicional:**O feedback dos sistemas de informação não fornece informações que permitiriam que indivíduos não autorizados comprometessem os mecanismos de autenticação. Para alguns tipos de sistemas de informação ou componentes de sistema, por exemplo, desktops / notebooks com monitores relativamente grandes, a ameaça (geralmente chamada de navegação no ombro) pode ser significativa. Para outros tipos de sistemas ou componentes, por exemplo, dispositivos móveis com telas de 2 a 4 polegadas, essa ameaça pode ser menos significativa e pode precisar ser equilibrada com a maior probabilidade de erros de entrada tipográfica devido aos pequenos teclados. Portanto, os meios para ocultar o feedback do autenticador são selecionados de acordo. Ocultar o feedback das informações de autenticação inclui, por exemplo, exibir asteriscos quando os usuários digitam senhas nos dispositivos de entrada ou exibir comentários por um tempo muito limitado antes de ocultá-las completamente.

## IA-7: Autenticação de Módulo Criptográfico (P1)

**Descrição do Controle:**O sistema de informações implementa mecanismos de autenticação em um módulo criptográfico que atendem aos requisitos das leis federais aplicáveis, ordens executivas, diretivas, diretivas, políticas, regulamentos, padrões e orientações para essa autenticação.  
  
**Guia Adicional:**Mecanismos de autenticação podem ser necessários dentro de um módulo criptográfico para autenticar um operador acessando o módulo e verificar se o operador está autorizado a assumir a função solicitada e executar serviços dentro dessa função.

**Referências:**

|  |  |
| --- | --- |
| Publicações de Normas Federais de Processamento de Informações N.140 | http://csrc.nist.gov/publications/PubsFIPS.html#140 |
| NIST - CSRC: Centro de Recursos de Segurança de Computadores | http://csrc.nist.gov/groups/STM/cmvp/index.html |

## IA-8: Identificação e Autenticação (Usuários Não Organizacionais) (P1)

**Descrição do Controle:**O sistema de informações identifica e autentica exclusivamente usuários não organizacionais (ou processos agindo em nome de usuários não organizacionais).  
  
**Guia Adicional:**Usuários não organizacionais incluem usuários do sistema de informações que não sejam usuários organizacionais explicitamente cobertos pelo IA-2. Esses indivíduos são identificados e autenticados exclusivamente para acessos diferentes daqueles explicitamente identificados e documentados no AC-14. De acordo com a iniciativa de governo eletrônico de autenticação eletrônica, a autenticação de usuários não organizacionais que acessam sistemas de informações federais pode ser necessária para proteger informações federais, proprietárias ou relacionadas à privacidade (com exceções observadas para sistemas de segurança nacional). As organizações usam avaliações de risco para determinar as necessidades de autenticação e consideram escalabilidade, praticidade e segurança ao equilibrar a necessidade de garantir facilidade de uso para acesso a informações e sistemas de informações federais com a necessidade de proteger e mitigar adequadamente os riscos. O IA-2 trata dos requisitos de identificação e autenticação para acesso aos sistemas de informação pelos usuários da organização.  
  
**Melhorias do Controle:**

### IA-8(1): Identificação e Autenticação (Usuários Não Organizacionais) | Aceitação de Credenciais PIV de Outras Agências

O sistema de informações aceita e verifica eletronicamente as credenciais de verificação de identidade pessoal (PIV) de outras agências federais.  
Guia Adicional: Esse aprimoramento de controle se aplica a sistemas de controle de acesso lógico (LACS) e sistemas de controle de acesso físico (PACS). As credenciais de verificação de identidade pessoal (PIV) são aquelas emitidas por agências federais que estão em conformidade com a publicação FIPS 201 e com os documentos de orientação. O Memorando OMB 11-11 exige que as agências federais continuem implementando os requisitos especificados no HSPD-12 para permitir o uso de credenciais de PIV em toda a agência.

### IA-8(2): Identificação e Autenticação (Usuários Não Organizacionais) | Aceitação de Credenciais de Terceiros

O sistema de informações aceita apenas credenciais de terceiros aprovadas pela FICAM.  
Guia Adicional: Esse aprimoramento de controle geralmente se aplica a sistemas de informações organizacionais acessíveis ao público em geral, por exemplo, sites voltados para o público. Credenciais de terceiros são aquelas emitidas por entidades governamentais não federais aprovadas pela iniciativa Trust Framework Solutions da Federal Identity, Credential and Access Management (FICAM). As credenciais de terceiros aprovadas atendem ou excedem o conjunto de requisitos mínimos técnicos, de segurança, privacidade e maturidade organizacional em todo o governo federal. Isso permite que as partes confiáveis do governo federal confiem nessas credenciais nos níveis de garantia aprovados.

### IA-8(3): Identificação e Autenticação (Usuários Não Organizacionais) | Utilização de Produtos Aprovados pela FICAM

O sistema de informação está em conformidade com os produtos aprovados pela FICAM.  
Guia Adicional: Esse aprimoramento de controle aborda os padrões abertos de gerenciamento de identidades. Para garantir que esses padrões sejam viáveis, robustos, confiáveis, sustentáveis (por exemplo, disponíveis em produtos comerciais de tecnologia da informação) e interoperáveis conforme documentado, o governo dos Estados Unidos avalia e escopo os padrões de gerenciamento de identidades e implementações de tecnologia em relação à legislação federal, diretrizes, políticas aplicáveis e requisitos. O resultado são perfis de implementação emitidos pela FICAM de protocolos aprovados (por exemplo, protocolos de autenticação da FICAM, como SAML 2.0 e OpenID 2.0, além de outros protocolos, como o FICAM Backend Attribute Exchange).

### IA-8(4): Identificação e Autenticação (Usuários Não Organizacionais) | Utilização de Perfis Aprovados pela FICAM

O sistema de informação está em conformidade com os perfis aprovados pela FICAM.  
Guia Adicional: Esse aprimoramento de controle aborda os padrões abertos de gerenciamento de identidades. Para garantir que esses padrões sejam viáveis, robustos, confiáveis, sustentáveis (por exemplo, disponíveis em produtos comerciais de tecnologia da informação) e interoperáveis conforme documentado, o governo dos Estados Unidos avalia e escopo os padrões de gerenciamento de identidades e implementações de tecnologia em relação à legislação federal, diretrizes, políticas aplicáveis e requisitos. O resultado são perfis de implementação emitidos pela FICAM de protocolos aprovados (por exemplo, protocolos de autenticação da FICAM, como SAML 2.0 e OpenID 2.0, além de outros protocolos, como o FICAM Backend Attribute Exchange).

### IA-8(5): Identificação e Autenticação (Usuários Não Organizacionais) | Aceitação de Credenciais PIV-I

O sistema de informações aceita e verifica eletronicamente as credenciais de Personal Identity Verification-I (PIV-I).  
Guia Adicional: Este aprimoramento de controle: (i) aplica-se a sistemas de controle de acesso lógico e físico; e (ii) aborda Emissores Não Federais (NFIs) de carteiras de identidade que desejam interoperar com os sistemas de informações de Verificação de Identidade Pessoal (PIV) do governo dos Estados Unidos e que podem ser confiáveis por terceiros dependentes do governo federal. A política de certificado X.509 para a Federal Bridge Certification Authority (FBCA) atende aos requisitos de PIV-I. O cartão PIV-I é adequado para o Nível de Garantia 4, conforme definido no Memorando OMB 04-04 e na Publicação Especial NIST 800-63, e na autenticação multifator conforme definido na Publicação Especial NIST 800-116. As credenciais PIV-I são aquelas emitidas por um provedor PIV-I cuja política de certificado PIV-I é mapeada para a Política de Certificação Federal Bridge PIV-I. Um provedor PIV-I é certificado cruzadamente (diretamente ou através de outra ponte PKI) com o FBCA com políticas que foram mapeadas e aprovadas como atendendo aos requisitos das políticas de PIV-I definidas na política de certificado do FBCA.

**Referências:**

|  |  |
| --- | --- |
| OMB Memorando 04-04 | https://georgewbush-whitehouse.archives.gov/omb/memoranda/fy04/m04-04.pdf |
| OMB Memorando 11-11 | https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2011/m11-11.pdf |
| FICAM - Roteiro e Orientação para Implementação | http://www.idmanagement.gov/documents/ficam-roadmap-and-implementation-guidance |
| Publicações de Normas Federais de Processamento de Informações N.201 | http://csrc.nist.gov/publications/PubsFIPS.html#201 |
| Publicação Especial NIST 800-63 | https://csrc.nist.gov/publications/search?keywords-lg=800-63 |
| Publicação Especial NIST 800-116 | https://csrc.nist.gov/publications/search?keywords-lg=800-116 |
| NIST - NSTIC: Estratégia Nacional para Identidades Confiáveis no Ciberespaço | http://www.nist.gov/nstic |
| FICAM: Identidade Federal, Credencial e Gerenciamento de Acesso | http://idmanagement.gov |

## IA-9: Identificação e Autenticação de Serviços (P0)

**Descrição do Controle:**A organização identifica e autentica [Atribuição: serviços do sistema de informações definidos pela organização] usando [Atribuição: salvaguardas de segurança definidas pela organização].  
  
**Guia Adicional:**Esse controle suporta arquiteturas orientadas a serviços e outras abordagens arquitetônicas distribuídas que exigem a identificação e autenticação de serviços do sistema de informações. Nessas arquiteturas, os serviços externos geralmente aparecem dinamicamente. Portanto, os sistemas de informação devem poder determinar de maneira dinâmica se provedores externos e serviços associados são autênticos. As salvaguardas implementadas pelos sistemas de informações organizacionais para validar a autenticidade do provedor e do serviço incluem, por exemplo, assinatura de informações ou códigos, gráficos de proveniência e/ou assinaturas eletrônicas indicando ou incluindo as fontes de serviços.  
  
**Melhorias do Controle:**

### IA-9(1): Identificação e Autenticação de Serviços | Intercâmbio de Informações

A organização garante que os provedores de serviços recebam, validem e transmitam informações de identificação e autenticação.

### IA-9(2): Identificação e Autenticação de Serviços | Transmissão de Decisões

A organização garante que as decisões de identificação e autenticação sejam transmitidas entre [Atribuição: serviços definidos pela organização] de acordo com as políticas da organização.  
Guia Adicional: Para arquiteturas distribuídas (por exemplo, arquiteturas orientadas a serviços), as decisões relacionadas à validação de declarações de identificação e autenticação podem ser tomadas por serviços separados dos serviços que atuam nessas decisões. Em tais situações, é necessário fornecer as decisões de identificação e autenticação (em oposição aos identificadores e autenticadores reais) aos serviços que precisam agir sobre essas decisões.

## IA-10: Identificação Adaptativa e Autenticação (P0)

**Descrição do Controle:**A organização exige que os indivíduos que acessam o sistema de informações empreguem [Atribuição: técnicas ou mecanismos de autenticação suplementar definidos pela organização] sob [Atribuição: circunstâncias ou situações definidas pela organização].  
  
**Guia Adicional:**Os adversários podem comprometer mecanismos de autenticação individuais e, posteriormente, tentar se passar por usuários legítimos. Essa situação pode ocorrer potencialmente com qualquer mecanismo de autenticação empregado pelas organizações. Para lidar com essa ameaça, as organizações podem empregar técnicas / mecanismos específicos e estabelecer protocolos para avaliar comportamentos suspeitos (por exemplo, indivíduos acessando informações que normalmente não acessam como parte de suas tarefas, funções ou responsabilidades normais, acessando quantidades maiores de informações do que as os indivíduos acessariam rotineiramente ou tentariam acessar informações de endereços de rede suspeitos). Nessas situações, quando certas condições ou gatilhos pré-estabelecidos ocorrem, as organizações podem exigir que indivíduos selecionados forneçam informações adicionais de autenticação. Outro uso potencial para identificação e autenticação adaptativa é aumentar a força do mecanismo com base no número e/ou tipos de registros acessados.

## IA-11: Re-Autenticação (P0)

**Descrição do Controle:**A organização exige que os usuários e os dispositivos sejam autenticados novamente quando [Atribuição: circunstâncias ou situações definidas pela organização que exijam nova autenticação].  
  
**Guia Adicional:**Além dos requisitos de re-autenticação associados aos bloqueios de sessão, as organizações podem exigir a re-autenticação de indivíduos e/ou dispositivos em outras situações, incluindo, por exemplo: (i) quando os autenticadores são alterados; (ii) quando os papéis mudam; (iii) quando as categorias de segurança dos sistemas de informação mudam; (iv) quando ocorre a execução de funções privilegiadas; (v) após um período fixo de tempo; ou (vi) periodicamente.

# IR - Resposta a Incidentes

## IR-1: Política e Procedimentos de Resposta a Incidentes (P1)

**Descrição do Controle:**A organização:  
  
a. Desenvolve, documenta e divulga para [Atribuição: pessoal ou funções definidas pela organização]:  
  
1. Uma política de resposta a incidentes que aborda finalidade, escopo, funções, responsabilidades, comprometimento gerencial, coordenação entre entidades organizacionais e conformidade; e  
  
2. Procedimentos para facilitar a implementação da política de resposta a incidentes e dos controles de resposta a incidentes associados; e  
  
b. Revisa e atualiza a atual:  
  
1. Política de resposta a incidentes [Atribuição: frequência definida pela organização]; e  
  
2. Procedimentos de resposta a incidentes [Tarefa: frequência definida pela organização].  
  
**Guia Adicional:**Esse controle trata do estabelecimento de políticas e procedimentos para a implementação efetiva de controles de segurança selecionados e aprimoramentos de controle na família de RI. As políticas e procedimentos refletem as leis federais aplicáveis, ordens executivas, diretivas, regulamentos, políticas, normas e diretrizes. Políticas e procedimentos do programa de segurança no nível da organização podem tornar desnecessária a necessidade de políticas e procedimentos específicos do sistema. A política pode ser incluída como parte da política geral de segurança da informação para organizações ou, inversamente, pode ser representada por múltiplas políticas refletindo a natureza complexa de certas organizações. Os procedimentos podem ser estabelecidos para o programa de segurança em geral e para sistemas de informação específicos, se necessário. A estratégia de gerenciamento de risco organizacional é um fator chave no estabelecimento de políticas e procedimentos.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-12 | https://csrc.nist.gov/publications/search?keywords-lg=800-12 |
| Publicação Especial NIST 800-61 | https://csrc.nist.gov/publications/search?keywords-lg=800-61 |
| Publicação Especial NIST 800-83 | https://csrc.nist.gov/publications/search?keywords-lg=800-83 |
| Publicação Especial NIST 800-100 | https://csrc.nist.gov/publications/search?keywords-lg=800-100 |

## IR-2: Treinamento de Resposta a Incidentes (P2)

**Descrição do Controle:**A organização fornece treinamento em resposta a incidentes para usuários do sistema de informações consistente com as funções e responsabilidades atribuídas:  
  
a. Dentro de [Atribuição: período definido pela organização] de assumir uma função ou responsabilidade de resposta a incidentes;  
  
b. Quando exigido pelas alterações do sistema de informação; e  
  
c. [Atribuição: frequência definida-organização] depois.  
  
**Guia Adicional:**O treinamento em resposta a incidentes fornecido pelas organizações está vinculado às funções e responsabilidades atribuídas do pessoal da organização para garantir que o conteúdo e o nível de detalhes apropriados sejam incluídos nesse treinamento. Por exemplo, usuários regulares podem precisar apenas saber para quem ligar ou como reconhecer um incidente no sistema de informações; os administradores de sistema podem exigir treinamento adicional sobre como lidar / corrigir incidentes; os responsáveis pela resposta a incidentes podem receber treinamento mais específico sobre forense, relatórios, recuperação e restauração do sistema. O treinamento de resposta a incidentes inclui o treinamento do usuário na identificação e relato de atividades suspeitas, tanto de fontes externas quanto internas.  
  
**Melhorias do Controle:**

### IR-2(1): Treinamento de Resposta a Incidentes | Eventos Simulados

A organização incorpora eventos simulados no treinamento de resposta a incidentes para facilitar a resposta eficaz do pessoal em situações de crise.

### IR-2(2): Treinamento de Resposta a Incidentes | Ambientes Automatizados de Formação

A organização emprega mecanismos automatizados para fornecer um ambiente de treinamento de resposta a incidentes mais completo e realista.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-16 | https://csrc.nist.gov/publications/search?keywords-lg=800-16 |
| Publicação Especial NIST 800-50 | https://csrc.nist.gov/publications/search?keywords-lg=800-50 |

## IR-3: Teste de Resposta a Incidentes (P2)

**Descrição do Controle:**A organização testa a capacidade de resposta a incidentes do sistema de informações [Atribuição: frequência definida pela organização] usando [Atribuição: testes definidos pela organização] para determinar a eficácia da resposta a incidentes e documenta os resultados.  
  
**Guia Adicional:**As organizações testam os recursos de resposta a incidentes para determinar a eficácia geral dos recursos e identificar possíveis pontos fracos ou deficiências. O teste de resposta a incidentes inclui, por exemplo, o uso de listas de verificação, exercícios de orientação ou de mesa, simulações (paralela / interrupção total) e exercícios abrangentes. O teste de resposta a incidentes também pode incluir uma determinação dos efeitos nas operações organizacionais (por exemplo, redução dos recursos da missão), ativos organizacionais e indivíduos devido à resposta a incidentes.  
  
**Melhorias do Controle:**

### IR-3(1): Teste de Resposta a Incidentes | Testes Automatizados

A organização emprega mecanismos automatizados para testar de maneira mais completa e eficaz a capacidade de resposta a incidentes.  
Guia Adicional: As organizações usam mecanismos automatizados para testar de maneira mais completa e eficaz os recursos de resposta a incidentes, por exemplo: (i) fornecendo uma cobertura mais completa dos problemas de resposta a incidentes; (ii) selecionando cenários e ambientes de teste mais realistas; e (iii) enfatizando a capacidade de resposta.

### IR-3(2): Teste de Resposta a Incidentes | Coordenação com Planos Relacionados

A organização coordena o teste de resposta a incidentes com os elementos organizacionais responsáveis pelos planos relacionados.  
Guia Adicional: Os planos organizacionais relacionados ao teste de resposta a incidentes incluem, por exemplo, Planos de Continuidade de Negócios, Planos de Contingência, Planos de Recuperação de Desastres, Planos de Continuidade de Operações, Planos de Comunicação de Crise, Planos de Infraestrutura Crítica e Planos de Emergência de Ocupantes.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-84 | https://csrc.nist.gov/publications/search?keywords-lg=800-84 |
| Publicação Especial NIST 800-115 | https://csrc.nist.gov/publications/search?keywords-lg=800-115 |

## IR-4: Manuseio de Incidentes (P1)

**Descrição do Controle:**A organização:  
  
a. Implementa um recurso de tratamento de incidentes para incidentes de segurança que inclui preparação, detecção e análise, contenção, erradicação e recuperação;  
  
b. Coordena atividades de manipulação de incidentes com atividades de planejamento de contingência; e  
  
c. Incorpora lições aprendidas de atividades de tratamento de incidentes em andamento em procedimentos de resposta a incidentes, treinamento e testes, e implementa as mudanças resultantes de acordo.  
  
**Guia Adicional:**As organizações reconhecem que a capacidade de resposta a incidentes depende da capacidade dos sistemas de informações organizacionais e dos processos de missão / negócios suportados por esses sistemas. Portanto, as organizações consideram a resposta a incidentes como parte da definição, design e desenvolvimento de processos de missão / negócios e sistemas de informação. Informações relacionadas a incidentes podem ser obtidas de uma variedade de fontes, incluindo, por exemplo, monitoramento de auditoria, monitoramento de rede, monitoramento de acesso físico, relatórios de usuário / administrador e eventos de cadeia de suprimentos relatados. A capacidade efetiva de tratamento de incidentes inclui a coordenação entre muitas entidades organizacionais, incluindo, por exemplo, proprietários de missão / empresa, proprietários de sistemas de informação, autoridades autorizadoras, escritórios de recursos humanos, escritórios de segurança física e de pessoal, departamentos jurídicos, pessoal de operações, escritórios de compras e o executivo de risco (função).  
  
**Melhorias do Controle:**

### IR-4(1): Manuseio de Incidentes | Processos Automatizados de Manuseio de Incidentes

A organização emprega mecanismos automatizados para apoiar o processo de tratamento de incidentes.  
Guia Adicional: Os mecanismos automatizados que suportam os processos de tratamento de incidentes incluem, por exemplo, sistemas de gerenciamento de incidentes online.

### IR-4(2): Manuseio de Incidentes | Reconfiguração Dinâmica

A organização inclui reconfiguração dinâmica de [Atribuição: componentes do sistema de informações definidos pela organização] como parte do recurso de resposta a incidentes.  
Guia Adicional: A reconfiguração dinâmica inclui, por exemplo, alterações nas regras do roteador, listas de controle de acesso, parâmetros do sistema de detecção / prevenção de intrusões e regras de filtro para firewalls e gateways. As organizações realizam reconfiguração dinâmica dos sistemas de informação, por exemplo, para interromper ataques, direcionar mal os atacantes e isolar componentes dos sistemas, limitando assim a extensão dos danos causados por violações ou comprometimentos. As organizações incluem prazos para alcançar a reconfiguração dos sistemas de informação na definição do recurso de reconfiguração, considerando a necessidade potencial de resposta rápida para lidar efetivamente com ameaças cibernéticas sofisticadas.

### IR-4(3): Manuseio de Incidentes | Continuidade de Operações

A organização identifica [Atribuição: classes de incidentes definidas pela organização] e [Atribuição: ações definidas pela organização a serem executadas em resposta a classes de incidentes] para garantir a continuação das missões organizacionais e funções de negócios.  
Guia Adicional: Classes de incidentes incluem, por exemplo, mau funcionamento devido a erros e omissões de design / implementação, ataques maliciosos direcionados e ataques maliciosos não direcionados. As ações de resposta a incidentes apropriadas incluem, por exemplo, degradação normal, desligamento do sistema de informações, retorno ao modo manual / tecnologia alternativa, na qual o sistema opera de maneira diferente, empregando medidas enganosas, fluxos de informações alternativos ou operando em um modo reservado exclusivamente para quando os sistemas estão sob ataque.

### IR-4(4): Manuseio de Incidentes | Correlação de Informação

A organização correlaciona informações de incidentes e respostas individuais a incidentes para obter uma perspectiva de toda a organização sobre a conscientização e resposta a incidentes.  
Guia Adicional: Às vezes, a natureza de um evento de ameaça, por exemplo, um ataque cibernético hostil, é tal que só pode ser observada reunindo informações de diferentes fontes, incluindo vários relatórios e procedimentos de relatório estabelecidos pelas organizações.

### IR-4(5): Manuseio de Incidentes | Desativação Automática do Sistema de Informação

A organização implementa um recurso configurável para desativar automaticamente o sistema de informações se [Atribuição: violações de segurança definidas pela organização] forem detectadas.

### IR-4(6): Manuseio de Incidentes | Ameaças Internacionais - Capacidades Específicas

A organização implementa a capacidade de tratamento de incidentes para ameaças internas.  
Guia Adicional: Embora muitas organizações tratem incidentes de ameaças internas como parte inerente de sua capacidade de resposta a incidentes organizacionais, esse aprimoramento de controle fornece ênfase adicional nesse tipo de ameaça e na necessidade de recursos específicos de tratamento de incidentes (conforme definido nas organizações) para fornecer respostas apropriadas e oportunas.

### IR-4(7): Manuseio de Incidentes | Ameaças Internacionais - Coordenação Entre Organizações

A organização coordena a capacidade de tratamento de incidentes para ameaças internas em [Atribuição: componentes ou elementos definidos pela organização].  
Guia Adicional: O tratamento de incidentes para ameaças internas (incluindo preparação, detecção e análise, contenção, erradicação e recuperação) requer uma coordenação estreita entre uma variedade de componentes ou elementos organizacionais para ser eficaz. Esses componentes ou elementos incluem, por exemplo, proprietários de missão / empresa, proprietários de sistemas de informação, escritórios de recursos humanos, escritórios de compras, escritórios de pessoal / segurança física, pessoal de operações e executivo de risco (função). Além disso, as organizações podem exigir apoio externo de órgãos federais, estaduais e locais de aplicação da lei.

### IR-4(8): Manuseio de Incidentes | Correlação com Organizações Externas

A organização coordena com [Atribuição: organizações externas definidas pela organização] para correlacionar e compartilhar [Atribuição: informações sobre incidentes definidas pela organização] para obter uma perspectiva entre organizações sobre o reconhecimento de incidentes e respostas mais eficazes a incidentes.  
Guia Adicional: A coordenação das informações sobre incidentes com organizações externas, incluindo, por exemplo, parceiros de missão / negócios, parceiros militares / coalizão, clientes e desenvolvedores de várias camadas, pode fornecer benefícios significativos. A coordenação entre organizações com relação ao tratamento de incidentes pode servir como um importante recurso de gerenciamento de riscos. Esse recurso permite que as organizações aproveitem informações críticas de várias fontes para responder efetivamente a incidentes relacionados à segurança das informações que afetam potencialmente as operações, ativos e indivíduos da organização.

### IR-4(9): Manuseio de Incidentes | Capacidade de Resposta Dinâmica

A organização emprega [Atribuição: recursos de resposta dinâmica definida pela organização] para responder efetivamente a incidentes de segurança.  
Guia Adicional: Esse aprimoramento de controle aborda a implantação de novos recursos de substituição ou em tempo hábil em resposta a incidentes de segurança (por exemplo, ações adversas durante ataques cibernéticos hostis). Isso inclui recursos implementados no nível da missão / processos de negócios (por exemplo, ativando processos alternativos de missão / negócios) e no nível do sistema de informação.

### IR-4(10): Manuseio de Incidentes | Coordenação da Cadeia de Fornecimento

A organização coordena as atividades de tratamento de incidentes que envolvem eventos da cadeia de suprimentos com outras organizações envolvidas na cadeia de suprimentos.  
Guia Adicional: As organizações envolvidas nas atividades da cadeia de suprimentos incluem, por exemplo, desenvolvedores de sistemas / produtos, integradores, fabricantes, empacotadores, montadores, distribuidores, fornecedores e revendedores. Os incidentes da cadeia de suprimentos incluem, por exemplo, comprometimentos / violações envolvendo componentes de sistemas de informação, produtos de tecnologia da informação, processos ou pessoal de desenvolvimento e processos de distribuição ou instalações de armazenamento.

**Referências:**

|  |  |
| --- | --- |
| Ordem Executiva da Casa Branca Nº13587 | http://www.whitehouse.gov/the-press-office/2011/10/07/executive-order-13587-structural-reforms-improve-security-classified-net |
| Publicação Especial NIST 800-61 | https://csrc.nist.gov/publications/search?keywords-lg=800-61 |

## IR-5: Monitoramento de Incidentes (P1)

**Descrição do Controle:**A organização rastreia e documenta incidentes de segurança do sistema de informações.  
  
**Guia Adicional:**A documentação de incidentes de segurança do sistema de informações inclui, por exemplo, a manutenção de registros sobre cada incidente, o status do incidente e outras informações pertinentes necessárias para forense, avaliando detalhes, tendências e manuseio do incidente. As informações sobre incidentes podem ser obtidas de várias fontes, incluindo, por exemplo, relatórios de incidentes, equipes de resposta a incidentes, monitoramento de auditoria, monitoramento de rede, monitoramento de acesso físico e relatórios de usuário / administrador.  
  
**Melhorias do Controle:**

### IR-5(1): Monitoramento de Incidentes | Rastreamento Automático / Coleta de Dados / Análise

A organização emprega mecanismos automatizados para auxiliar no rastreamento de incidentes de segurança e na coleta e análise de informações de incidentes.  
Guia Adicional: Mecanismos automatizados para rastrear incidentes de segurança e coletar / analisar informações de incidentes incluem, por exemplo, o dispositivo de monitoramento de rede Einstein e o monitoramento online de Centros de Resposta a Incidentes de Computador (CIRCs) ou outros bancos de dados eletrônicos de incidentes.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-61 | https://csrc.nist.gov/publications/search?keywords-lg=800-61 |

## IR-6: Relatórios de Incidentes (P1)

**Descrição do Controle:**A organização:  
  
a. Requer que a equipe relate denúncias de incidentes de segurança suspeitos ao recurso de resposta a incidentes organizacionais dentro de [Atribuição: período definido pela organização]; e  
  
b. Relata informações de incidentes de segurança para [Atribuição: autoridades definidas pela organização].  
  
**Guia Adicional:**A intenção desse controle é atender tanto aos requisitos específicos de relatório de incidentes dentro de uma organização quanto aos requisitos formais de relatório de incidentes para agências federais e suas organizações subordinadas. Incidentes de segurança suspeitos incluem, por exemplo, o recebimento de comunicações por e-mail suspeitas que podem potencialmente conter código malicioso. Os tipos de incidentes de segurança relatados, o conteúdo e a pontualidade dos relatórios e as autoridades de relatório designadas refletem as leis federais aplicáveis, ordens executivas, diretrizes, regulamentos, políticas, normas e orientações. A política federal atual exige que todas as agências federais (a menos que especificamente isentas de tais requisitos) relatem incidentes de segurança à Equipe de Prontidão de Emergência em Computador dos Estados Unidos (US-CERT) dentro dos prazos especificados no Conceito de Operações dos EUA-CERT para o Incidente Federal de Segurança Cibernética Manipulação.  
  
**Melhorias do Controle:**

### IR-6(1): Relatórios de Incidentes | Relatórios Automatizados

A organização emprega mecanismos automatizados para auxiliar no relato de incidentes de segurança.

### IR-6(2): Relatórios de Incidentes | Vulnerabilidades Relativas aos Incidentes

A organização relata vulnerabilidades do sistema de informações associadas a incidentes de segurança relatados para [Atribuição: pessoal ou funções definidas pela organização].

### IR-6(3): Relatórios de Incidentes | Coordenação com Cadeia de Fornecimento

A organização fornece informações sobre incidentes de segurança a outras organizações envolvidas na cadeia de suprimentos para sistemas de informações ou componentes de sistemas de informações relacionados ao incidente.  
Guia Adicional: As organizações envolvidas nas atividades da cadeia de suprimentos incluem, por exemplo, desenvolvedores de sistemas / produtos, integradores, fabricantes, empacotadores, montadores, distribuidores, fornecedores e revendedores. Os incidentes da cadeia de suprimentos incluem, por exemplo, comprometimentos / violações envolvendo componentes de sistemas de informação, produtos de tecnologia da informação, processos ou pessoal de desenvolvimento e processos de distribuição ou instalações de armazenamento. As organizações determinam as informações apropriadas para compartilhar, considerando o valor obtido com o apoio de organizações externas com o potencial de causar danos, devido à divulgação de informações confidenciais a organizações externas, que talvez tenham uma confiabilidade questionável.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-61 | https://csrc.nist.gov/publications/search?keywords-lg=800-61 |
| US-CERT: Equipe de Prontidão de Emergência do Computador dos Estados Unidos | http://www.us-cert.gov |

## IR-7: Assistência à Resposta a Incidentes (P2)

**Descrição do Controle:**A organização fornece um recurso de suporte à resposta a incidentes, parte integrante do recurso de resposta a incidentes organizacionais, que oferece consultoria e assistência aos usuários do sistema de informações para o manuseio e a comunicação de incidentes de segurança.  
  
**Guia Adicional:**Os recursos de suporte à resposta a incidentes fornecidos pelas organizações incluem, por exemplo, serviços de assistência, grupos de assistência e acesso a serviços forenses, quando necessário.  
  
**Melhorias do Controle:**

### IR-7(1): Assistência à Resposta a Incidentes | Suporte de Automação para Disponibilidade de Informação / Suporte

A organização emprega mecanismos automatizados para aumentar a disponibilidade de informações e suporte relacionados a respostas a incidentes.  
Guia Adicional: Mecanismos automatizados podem fornecer um recurso de envio e/ou recebimento para os usuários obterem assistência em resposta a incidentes. Por exemplo, os indivíduos podem ter acesso a um site para consultar o recurso de assistência ou, inversamente, o recurso de assistência pode enviar pro ativamente informações aos usuários (distribuição geral ou direcionadas) como parte da crescente compreensão dos recursos e suporte de resposta atuais.

### IR-7(2): Assistência à Resposta a Incidentes | Coordenação com Fornecedores Externos

A organização:  
  
a. Estabelece um relacionamento direto e cooperativo entre sua capacidade de resposta a incidentes e fornecedores externos de capacidade de proteção de sistemas de informação; e  
  
b. Identifica os membros da equipe de resposta a incidentes organizacionais para os fornecedores externos.  
Guia Adicional: Os provedores externos de capacidade de proteção do sistema de informação incluem, por exemplo, o programa Computer Network Defense dentro do Departamento de Defesa dos EUA. Fornecedores externos ajudam a proteger, monitorar, analisar, detectar e responder a atividades não autorizadas nos sistemas e redes de informações organizacionais.

## IR-8: Plano de Resposta a Incidentes (P1)

**Descrição do Controle:**A organização:  
  
a. Desenvolve um plano de resposta a incidentes que:  
  
1. Fornece à organização um roteiro para implementar sua capacidade de resposta a incidentes;  
  
2. Descreve a estrutura e organização da capacidade de resposta a incidentes;  
  
3. Fornece uma abordagem de alto nível sobre como a capacidade de resposta a incidentes se encaixa na organização geral;  
  
4. Atende aos requisitos exclusivos da organização, relacionados à missão, tamanho, estrutura e funções;  
  
5. Define incidentes reportáveis;  
  
6. Fornece métricas para medir a capacidade de resposta a incidentes dentro da organização;  
  
7. Define os recursos e o suporte de gerenciamento necessários para efetivamente manter e amadurecer uma capacidade de resposta a incidentes; e  
  
8. É revisado e aprovado por [Designação: pessoal ou funções definidas pela organização];  
  
b. Distribui cópias do plano de resposta a incidentes para [Atribuição: pessoal de resposta a incidentes definido pela organização (identificado por nome e/ou função) e elementos organizacionais];  
  
c. Revisa o plano de resposta a incidentes [Tarefa: frequência definida pela organização];  
  
d. Atualiza o plano de resposta a incidentes para solucionar alterações ou problemas do sistema / organização encontrados durante a implementação, execução ou teste do plano;  
  
e. Comunica alterações no plano de resposta a incidentes em [Atribuição: pessoal de resposta a incidentes definido pela organização (identificado por nome e/ou função) e elementos organizacionais]; e  
  
f. Protege o plano de resposta a incidentes de divulgação e modificação não autorizadas.  
  
**Guia Adicional:**É importante que as organizações desenvolvam e implementem uma abordagem coordenada da resposta a incidentes. Missões organizacionais, funções comerciais, estratégias, metas e objetivos para resposta a incidentes ajudam a determinar a estrutura dos recursos de resposta a incidentes. Como parte de uma capacidade abrangente de resposta a incidentes, as organizações consideram a coordenação e o compartilhamento de informações com organizações externas, incluindo, por exemplo, provedores de serviços externos e organizações envolvidas na cadeia de suprimentos para sistemas de informações organizacionais.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-61 | https://csrc.nist.gov/publications/search?keywords-lg=800-61 |

## IR-9: Resposta ao Vazamento de Informação (P0)

**Descrição do Controle:**A organização responde a derramamentos de informações:  
  
a. Identificar as informações específicas envolvidas na contaminação do sistema de informação;  
  
b. Alerta [Designação: pessoal ou funções definidas pela organização] do vazamento de informações usando um método de comunicação não associado ao vazamento;  
  
c. Isolar o sistema de informações ou componente de sistema contaminado;  
  
d. Erradicar as informações do sistema ou componente de informações contaminadas;  
  
e. Identificar outros sistemas de informação ou componentes do sistema que possam ter sido subsequentemente contaminados; e  
  
f. Executando outras [Tarefas: ações definidas pela organização].  
  
**Guia Adicional:**O vazamento de informações refere-se a casos em que informações classificadas ou confidenciais são inadvertidamente colocadas em sistemas de informações que não estão autorizados a processar tais informações. Esses vazamentos de informações geralmente ocorrem quando informações inicialmente consideradas de menor sensibilidade são transmitidas para um sistema de informações e, em seguida, são determinadas como de maior sensibilidade. Nesse ponto, é necessária uma ação corretiva. A natureza da resposta organizacional geralmente é baseada no grau de sensibilidade das informações derramadas (por exemplo, categoria de segurança ou nível de classificação), os recursos de segurança do sistema de informações, a natureza específica da mídia de armazenamento contaminada e as autorizações de acesso (por exemplo, autorizações de segurança) de indivíduos com acesso autorizado ao sistema contaminado. Os métodos usados para comunicar informações sobre o derramamento após o fato não envolvem métodos diretamente associados ao derramamento real para minimizar o risco de espalhar ainda mais a contaminação antes que essa contaminação seja isolada e erradicada.  
  
**Melhorias do Controle:**

### IR-9(1): Resposta ao Vazamento de Informação | Pessoal Responsável

A organização atribui [Atribuição: pessoal ou funções definidas pela organização] com a responsabilidade de responder a derramamentos de informações.

### IR-9(2): Resposta ao Vazamento de Informação | Treinamento

A organização fornece treinamento em resposta a derramamento de informação [Tarefa: frequência definida pela organização].

### IR-9(3): Resposta ao Vazamento de Informação | Operações Pós-Derramamento

A organização implementa [Atribuição: procedimentos definidos pela organização] para garantir que o pessoal da organização impactado por vazamentos de informações possa continuar a executar tarefas atribuídas enquanto os sistemas contaminados estão realizando ações corretivas.  
Guia Adicional: Ações de correção para sistemas de informação contaminados devido a derramamentos de informações podem consumir muito tempo. Durante esses períodos, o pessoal pode não ter acesso aos sistemas contaminados, o que pode afetar sua capacidade de conduzir os negócios da organização.

### IR-9(4): Resposta ao Vazamento de Informação | Exposição a Pessoal Não Autorizado

A organização emprega [Atribuição: salvaguardas de segurança definidas pela organização] para o pessoal exposto a informações fora das autorizações de acesso atribuídas.  
Guia Adicional: As salvaguardas de segurança incluem, por exemplo, conscientizar o pessoal exposto a informações derramadas sobre as leis, diretrizes, políticas e/ou regulamentos federais sobre as informações e as restrições impostas com base na exposição a essas informações.

## IR-10: Equipe Integrada de Análise da Segurança da Informação (P0)

**Descrição do Controle:**A organização estabelece uma equipe integrada de analistas de códigos forenses / maliciosos, desenvolvedores de ferramentas e equipe de operações em tempo real.  
  
**Guia Adicional:**Ter uma equipe integrada para resposta a incidentes facilita o compartilhamento de informações. Essa capacidade permite que o pessoal da organização, incluindo desenvolvedores, implementadores e operadores, aproveite o conhecimento da equipe sobre a ameaça, a fim de implementar medidas defensivas que permitirão às organizações deter mais eficazmente as invasões. Além disso, promove a rápida detecção de intrusões, o desenvolvimento de mitigações apropriadas e a implantação de medidas defensivas eficazes. Por exemplo, quando uma invasão é detectada, a equipe de análise de segurança integrada pode desenvolver rapidamente uma resposta apropriada para os operadores implementarem, correlacionar o novo incidente com informações sobre invasões passadas e aumentar o desenvolvimento contínuo da inteligência. Isso permite que a equipe identifique TTPs adversários que estejam vinculados ao andamento das operações ou a missões / funções de negócios específicas e defina ações responsivas de uma maneira que não perturbe as operações da missão / negócios. Idealmente, as equipes de análise de segurança da informação são distribuídas nas organizações para tornar a capacidade mais resiliente.

# MA - Manutenção

## MA-1: Política e Procedimentos da Manutenção de Sistemas (P1)

**Descrição do Controle:**A organização:  
  
a. Desenvolve, documenta e divulga para [Atribuição: pessoal ou funções definidas pela organização]:  
  
1. Uma política de manutenção do sistema que atenda a finalidade, escopo, funções, responsabilidades, compromisso de gerenciamento, coordenação entre entidades organizacionais e conformidade; e  
  
2. Procedimentos para facilitar a implementação da política de manutenção do sistema e dos controles de manutenção do sistema associados; e  
  
b. Revisa e atualiza a atual:  
  
1. Política de manutenção do sistema [Atribuição: frequência definida pela organização]; e  
  
2. Procedimentos de manutenção do sistema [Atribuição: frequência definida pela organização].  
  
**Guia Adicional:**Esse controle aborda o estabelecimento de políticas e procedimentos para a implementação efetiva de controles de segurança selecionados e aprimoramentos de controle na família MA. As políticas e procedimentos refletem as leis federais aplicáveis, ordens executivas, diretivas, regulamentos, políticas, normas e diretrizes. Políticas e procedimentos do programa de segurança no nível da organização podem tornar desnecessária a necessidade de políticas e procedimentos específicos do sistema. A política pode ser incluída como parte da política geral de segurança da informação para organizações ou, inversamente, pode ser representada por múltiplas políticas refletindo a natureza complexa de certas organizações. Os procedimentos podem ser estabelecidos para o programa de segurança em geral e para sistemas de informação específicos, se necessário. A estratégia de gerenciamento de risco organizacional é um fator chave no estabelecimento de políticas e procedimentos.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-12 | https://csrc.nist.gov/publications/search?keywords-lg=800-12 |
| Publicação Especial NIST 800-100 | https://csrc.nist.gov/publications/search?keywords-lg=800-100 |

## MA-2: Manutenção Controlada (P2)

**Descrição do Controle:**A organização:  
  
a. Programa, executa, documenta e revisa registros de manutenção e reparos nos componentes do sistema de informações, de acordo com as especificações do fabricante ou fornecedor e/ou requisitos organizacionais;  
  
b. Aprova e monitora todas as atividades de manutenção, sejam realizadas no local ou remotamente, e se o equipamento é reparado no local ou removido para outro local;  
  
c. Requer que [Atribuição: pessoal ou funções definidas pela organização] aprove explicitamente a remoção do sistema de informação ou dos componentes do sistema das instalações da organização para manutenção ou reparos externos;  
  
d. Higieniza o equipamento para remover todas as informações da mídia associada antes da remoção das instalações da organização para manutenção ou reparos externos;  
  
e. Verifica todos os controles de segurança potencialmente afetados para verificar se os controles ainda estão funcionando corretamente após ações de manutenção ou reparo; e  
  
f. Inclui [Atribuição: informações relacionadas à manutenção definida pela organização] nos registros de manutenção organizacional.  
  
**Guia Adicional:**Esse controle aborda os aspectos de segurança das informações do programa de manutenção do sistema de informações e se aplica a todos os tipos de manutenção de qualquer componente do sistema (incluindo aplicativos) realizado por qualquer entidade local ou não local (por exemplo, contrato, garantia, internamente, manutenção de software acordo). A manutenção do sistema também inclui os componentes não diretamente associados ao processamento de informações e/ou retenção de dados / informações, como scanners, copiadoras e impressoras. As informações necessárias para a criação de registros de manutenção eficazes incluem, por exemplo: (i) data e hora da manutenção; (ii) nome dos indivíduos ou grupo que realiza a manutenção; (iii) nome da escolta, se necessário; (iv) uma descrição da manutenção realizada; e (v) componentes / equipamentos do sistema de informação removidos ou substituídos (incluindo números de identificação, se aplicável). O nível de detalhe incluído nos registros de manutenção pode ser informado pelas categorias de segurança dos sistemas de informações organizacionais. As organizações consideram os problemas da cadeia de suprimentos associados aos componentes de substituição para sistemas de informação.  
  
**Melhorias do Controle:**

### MA-2(1): Manutenção Controlada | Conteúdo do Registro

[Retirado: Incorporado no MA-2].

### MA-2(2): Manutenção Controlada | Atividades de Manutenção Automatizadas

A organização:  
  
a. Emprega mecanismos automatizados para agendar, conduzir e documentar a manutenção e reparos; e  
  
b. Produz registros atualizados, precisos e completos de todas as ações de manutenção e reparo solicitadas, agendadas, em processo e concluídas.

## MA-3: Ferramentas de Manutenção (P3)

**Descrição do Controle:**A organização aprova, controla e monitora as ferramentas de manutenção do sistema de informações.  
  
**Guia Adicional:**Esse controle soluciona problemas relacionados à segurança associados a ferramentas de manutenção usadas especificamente para ações de diagnóstico e reparo em sistemas de informações organizacionais. As ferramentas de manutenção podem incluir itens de hardware, software e firmware. As ferramentas de manutenção são veículos em potencial para o transporte de código malicioso, intencional ou involuntariamente, para uma instalação e posteriormente para os sistemas de informações organizacionais. As ferramentas de manutenção podem incluir, por exemplo, equipamento de teste de diagnóstico de hardware / software e farejadores de pacotes de hardware / software. Esse controle não cobre componentes de hardware / software que podem oferecer suporte à manutenção do sistema de informações, mas faz parte do sistema, por exemplo, o software que implementa "ping", "ls", "ipconfig" ou o hardware e software que implementa o monitoramento porta de um comutador Ethernet.  
  
**Melhorias do Controle:**

### MA-3(1): Ferramentas de Manutenção | Ferramentas de Inspeção

A organização inspeciona as ferramentas de manutenção transportadas pelas instalações pelo pessoal de manutenção quanto a modificações impróprias ou não autorizadas.  
Guia Adicional: Se, após a inspeção das ferramentas de manutenção, as organizações determinarem que as ferramentas foram modificadas de maneira inadequada / não autorizada ou contiverem códigos maliciosos, o incidente será tratado de acordo com as políticas e procedimentos organizacionais para o tratamento de incidentes.

### MA-3(2): Ferramentas de Manutenção | Inspeção de Mídia

A organização verifica a mídia que contém programas de diagnóstico e teste em busca de códigos maliciosos antes que a mídia seja usada no sistema de informações.  
Guia Adicional: Se, após a inspeção da mídia que contém programas de diagnóstico e teste de manutenção, as organizações determinarem que a mídia contém código malicioso, o incidente será tratado de acordo com as políticas e procedimentos organizacionais de tratamento de incidentes.

### MA-3(3): Ferramentas de Manutenção | Impedir Remoção Não Autorizada

A organização impede a remoção não autorizada de equipamentos de manutenção contendo informações organizacionais:  
  
a. Verificar se não há informações organizacionais contidas no equipamento;  
  
b. Higienizar ou destruir o equipamento;  
  
c. Reter o equipamento dentro da instalação; ou  
  
d. Obtenção de uma isenção de [Atribuição: pessoal ou funções definidas pela organização] autorizando explicitamente a remoção do equipamento da instalação.

### MA-3(4): Ferramentas de Manutenção | Uso Restrito de Ferramentas

O sistema de informações restringe o uso de ferramentas de manutenção apenas ao pessoal autorizado.  
Guia Adicional: Este aprimoramento de controle se aplica a sistemas de informação que são usados para executar funções de manutenção.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-88 | https://csrc.nist.gov/publications/search?keywords-lg=800-88 |

## MA-4: Manutenção Não Local (P2)

**Descrição do Controle:**A organização:  
  
a. Aprova e monitora atividades de diagnóstico e manutenção não-local;  
  
b. Permite o uso de ferramentas de diagnóstico e manutenção não-locais apenas de forma consistente com a política organizacional e documentada no plano de segurança do sistema de informações;  
  
c. Emprega autenticadores fortes no estabelecimento de sessões de manutenção e diagnóstico não-locais;  
  
d. Mantém registros de manutenção não local e atividades de diagnóstico; e  
  
e. Encerra a sessão e as conexões de rede quando a manutenção não local é concluída.  
  
**Guia Adicional:**Atividades de diagnóstico e manutenção não-local são aquelas realizadas por indivíduos que se comunicam através de uma rede, seja uma rede externa (por exemplo, a Internet) ou uma rede interna. As atividades locais de manutenção e diagnóstico são aquelas realizadas por indivíduos fisicamente presentes no sistema de informações ou componente do sistema de informações e que não se comunicam através de uma conexão de rede. As técnicas de autenticação usadas no estabelecimento de sessões não locais de manutenção e diagnóstico refletem os requisitos de acesso à rede no IA-2. Normalmente, a autenticação forte exige autenticadores que são resistentes a ataques de repetição e empregam autenticação multifator. Autenticadores fortes incluem, por exemplo, PKI em que os certificados são armazenados em um token protegido por senha, frase secreta ou biométrica. A aplicação dos requisitos no MA-4 é cumprida em parte por outros controles.  
  
**Melhorias do Controle:**

### MA-4(1): Manutenção Não Local | Auditoria e Revisão

A organização:  
  
a. Audita sessões de diagnóstico e manutenção não local [Atribuição: eventos de auditoria definidos pela organização]; e  
  
b. Revisa os registros das sessões de manutenção e diagnóstico.

### MA-4(2): Manutenção Não Local | Manutenção Não Local do Documento

A organização documenta no plano de segurança do sistema de informações, as políticas e procedimentos para o estabelecimento e uso de manutenção não local e conexões de diagnóstico.

### MA-4(3): Manutenção Não Local | Segurança / Sanitização Comparáveis

A organização:  
  
a. Requer que serviços de diagnóstico e manutenção não-locais sejam executados a partir de um sistema de informações que implemente um recurso de segurança comparável ao recurso implementado no sistema que está sendo atendido; ou  
  
b. Remove o componente a ser reparado do sistema de informações antes da manutenção não-local ou dos serviços de diagnóstico, higieniza o componente (com relação às informações da organização) antes da remoção das instalações da organização e, após a execução do serviço, inspeciona e higieniza o componente (com relação à software potencialmente malicioso) antes de reconectar o componente ao sistema de informações.  
Guia Adicional: A capacidade de segurança comparável em sistemas de informação, ferramentas de diagnóstico e equipamentos que fornecem serviços de manutenção implica que os controles de segurança implementados nesses sistemas, ferramentas e equipamentos sejam pelo menos tão abrangentes quanto os controles no sistema de informações que está sendo atendido.

### MA-4(4): Manutenção Não Local | Autenticação / Separação de Sessões de Manutenção

A organização protege sessões de manutenção não-local por:  
  
a. Empregando [Atribuição: autenticadores definidos pela organização que são resistentes à reprodução]; e  
  
b. Separando as sessões de manutenção de outras sessões da rede com o sistema de informações por um ou outro.

### MA-4(5): Manutenção Não Local | Aprovações e Notificações

A organização:  
  
a. Requer a aprovação de cada sessão de manutenção não local por [Atribuição: pessoal ou funções definidas pela organização]; e  
  
b. Notifica [Atribuição: pessoal ou funções definidas pela organização] da data e hora da manutenção não local planejada.  
Guia Adicional: A notificação pode ser realizada pelo pessoal de manutenção. A aprovação de sessões de manutenção não-local é realizada pelo pessoal da organização, com suficiente segurança da informação e conhecimento do sistema de informação para determinar a adequação da manutenção proposta.

### MA-4(6): Manutenção Não Local | Proteção Criptográfica

O sistema de informações implementa mecanismos criptográficos para proteger a integridade e a confidencialidade das comunicações não locais de manutenção e diagnóstico.

### MA-4(7): Manutenção Não Local | Verificação de Desconexão Remota

O sistema de informações implementa a verificação de desconexão remota no final das sessões de manutenção e diagnóstico não-locais.  
Guia Adicional: A verificação de desconexão remota garante que as conexões remotas das sessões de manutenção não local tenham sido encerradas e não estejam mais disponíveis para uso.

**Referências:**

|  |  |
| --- | --- |
| Publicações de Normas Federais de Processamento de Informações N.140-2 | http://csrc.nist.gov/publications/PubsFIPS.html#140-2 |
| Publicações de Normas Federais de Processamento de Informações N.197 | http://csrc.nist.gov/publications/PubsFIPS.html#197 |
| Publicações de Normas Federais de Processamento de Informações N.201 | http://csrc.nist.gov/publications/PubsFIPS.html#201 |
| Publicação Especial NIST 800-63 | https://csrc.nist.gov/publications/search?keywords-lg=800-63 |
| Publicação Especial NIST 800-88 | https://csrc.nist.gov/publications/search?keywords-lg=800-88 |
| CNSS - Apólice 15 | https://www.cnss.gov/policies.html |

## MA-5: Manutenção Pessoal (P2)

**Descrição do Controle:**A organização:  
  
a. Estabelece um processo para autorização do pessoal de manutenção e mantém uma lista de organizações ou pessoal de manutenção autorizado;  
  
b. Garante que pessoas não acompanhadas que realizam manutenção no sistema de informações tenham exigido autorizações de acesso; e  
  
c. Designa pessoal organizacional com autorizações de acesso necessárias e competência técnica para supervisionar as atividades de manutenção de pessoas que não possuem as autorizações de acesso necessárias.  
  
**Guia Adicional:**Esse controle se aplica a indivíduos que realizam manutenção de hardware ou software em sistemas de informações organizacionais, enquanto o PE-2 aborda o acesso físico a indivíduos cujas tarefas de manutenção os colocam dentro do perímetro de proteção física dos sistemas (por exemplo, pessoal de custódia, pessoal de manutenção da fábrica). A competência técnica de supervisionar indivíduos refere-se à manutenção realizada nos sistemas de informação, enquanto as autorizações de acesso necessárias se referem à manutenção nos sistemas e nos seus arredores. Indivíduos não identificados anteriormente como pessoal de manutenção autorizado, como fabricantes de tecnologia da informação, fornecedores, integradores de sistemas e consultores, podem exigir acesso privilegiado aos sistemas de informações organizacionais, por exemplo, quando necessário para realizar atividades de manutenção com pouco ou nenhum aviso prévio. Com base nas avaliações organizacionais de risco, as organizações podem emitir credenciais temporárias para esses indivíduos. As credenciais temporárias podem ser usadas uma vez ou por períodos muito limitados.  
  
**Melhorias do Controle:**

### MA-5(1): Manutenção Pessoal | Indivíduos Sem Acesso Apropriado

A organização:  
  
a. Implementa procedimentos para o uso de pessoal de manutenção que não possui as devidas autorizações de segurança ou não são cidadãos dos EUA, que incluem os seguintes requisitos:  
  
b. Desenvolve e implementa salvaguardas de segurança alternativas no caso de um componente do sistema de informações não poder ser higienizado, removido ou desconectado do sistema.  
Guia Adicional: Esse aprimoramento de controle nega aos indivíduos que não possuem as devidas autorizações de segurança (ou seja, indivíduos que não possuem autorizações de segurança ou possuem autorizações de segurança em um nível inferior ao necessário) ou que não são cidadãos dos EUA, acesso visual e eletrônico a qualquer informação classificada, informações não classificadas controladas (CUI) ou qualquer outra informação confidencial contida nos sistemas de informações organizacionais. Os procedimentos para o uso da equipe de manutenção podem ser documentados nos planos de segurança dos sistemas de informação.

### MA-5(2): Manutenção Pessoal | Garantias de Segurança para Sistemas Classificados

A organização garante que o pessoal que realiza atividades de manutenção e diagnóstico em um sistema de informações que processa, armazena ou transmite informações classificadas possua autorizações de segurança e aprovações formais de acesso para pelo menos o nível mais alto de classificação e para todos os compartimentos de informações no sistema.

### MA-5(3): Manutenção Pessoal | Requisitos de Cidadania para Sistemas Classificados

A organização garante que o pessoal que realiza atividades de manutenção e diagnóstico em um sistema de informações que processa, armazena ou transmite informações classificadas seja cidadão dos EUA.

### MA-5(4): Manutenção Pessoal | Cidadãos Estrangeiros

A organização garante que:  
  
a. Nacionais estrangeiros autorizados (ou seja, estrangeiros com habilitações de segurança apropriadas) são usados para realizar atividades de manutenção e diagnóstico em sistemas de informações classificadas somente quando os sistemas pertencem e são operados em conjunto pelos Estados Unidos e governos aliados estrangeiros ou pertencentes e operados exclusivamente por governos aliados estrangeiros; e  
  
b. Aprovações, consentimentos e condições operacionais detalhadas relativas ao uso de estrangeiros para realizar atividades de manutenção e diagnóstico em sistemas de informação classificados estão totalmente documentadas nos Memorandos de Contratos.

### MA-5(5): Manutenção Pessoal | Manutenção Não Relacionada a Sistemas

A organização garante que o pessoal não escoltado que executa atividades de manutenção não diretamente associadas ao sistema de informações, mas na proximidade física do sistema, tenha exigido autorizações de acesso.  
Guia Adicional: O pessoal que realiza atividades de manutenção em outras capacidades não diretamente relacionadas ao sistema de informações inclui, por exemplo, pessoal físico da fábrica e pessoal de limpeza.

## MA-6: Manutenção Programada (P2)

**Descrição do Controle:**A organização obtém suporte de manutenção e/ou peças de reposição para [Atribuição: componentes do sistema de informações definidos pela organização] dentro de [Atribuição: período definido pela organização] da falha.  
  
**Guia Adicional:**As organizações especificam os componentes do sistema de informações que resultam em maior risco para operações e ativos organizacionais, indivíduos, outras organizações ou a Nação quando a funcionalidade fornecida por esses componentes não está operacional. As ações organizacionais para obter suporte de manutenção geralmente incluem a contratação de contratos adequados.  
  
**Melhorias do Controle:**

### MA-6(1): Manutenção Programada | Manutenção Preventiva

A organização executa manutenção preventiva em [Atribuição: componentes do sistema de informações definidos pela organização] em [Atribuição: intervalos de tempo definidos pela organização].  
Guia Adicional: A manutenção preventiva inclui cuidados proativos e manutenção de componentes de sistemas de informações organizacionais com o objetivo de manter equipamentos e instalações em condições operacionais satisfatórias. Essa manutenção fornece a inspeção sistemática, testes, medições, ajustes, substituição de peças, detecção e correção de falhas incipientes antes que elas ocorram ou antes que elas se transformem em grandes defeitos. O objetivo principal da manutenção preventiva é evitar / mitigar as consequências de falhas no equipamento. A manutenção preventiva foi projetada para preservar e restaurar a confiabilidade do equipamento, substituindo os componentes gastos antes que eles realmente falhem. Os métodos para determinar quais políticas de gerenciamento de falhas preventivas (ou outras) a serem aplicadas incluem, por exemplo, recomendações do fabricante do equipamento original (OEM), registros estatísticos de falhas, requisitos de códigos, legislação ou regulamentos dentro de uma jurisdição, opinião de especialistas, manutenção que já realizados em equipamentos semelhantes ou valores medidos e indicações de desempenho.

### MA-6(2): Manutenção Programada | Manutenção Preditiva

A organização executa manutenção preditiva em [Atribuição: componentes do sistema de informações definidos pela organização] em [Atribuição: intervalos de tempo definidos pela organização].  
Guia Adicional: A manutenção preditiva ou manutenção baseada em condições tenta avaliar a condição do equipamento executando um monitoramento periódico ou contínuo (online) das condições do equipamento. O objetivo da manutenção preditiva é realizar a manutenção em um momento programado em que a atividade de manutenção é mais econômica e antes que o equipamento perca o desempenho dentro de um limite. O componente preditivo da manutenção preditiva decorre do objetivo de prever a tendência futura da condição do equipamento. Essa abordagem usa princípios de controle estatístico de processos para determinar em que momento as atividades de manutenção futuras serão apropriadas. A maioria das inspeções preditivas de manutenção é realizada enquanto o equipamento está em serviço, minimizando a interrupção das operações normais do sistema. A manutenção preditiva pode resultar em economia substancial de custos e maior confiabilidade do sistema. A manutenção preditiva tende a incluir a medição do item. Para avaliar a condição do equipamento, a manutenção preditiva utiliza tecnologias de teste não destrutivas, como infravermelho, acústico (descarga parcial e ultrassônica no ar), detecção de coroa, análise de vibração, medições de nível sonoro, análise de óleo e outros testes online específicos.

### MA-6(3): Manutenção Programada | Suporte Automatizado para Manutenção Preditiva

A organização emprega mecanismos automatizados para transferir dados de manutenção preditiva para um sistema de gerenciamento de manutenção computadorizado.  
Guia Adicional: Um sistema informatizado de gerenciamento de manutenção mantém um banco de dados informatizado sobre as operações de manutenção das organizações e automatiza os dados de condição dos equipamentos de processamento para acionar o planejamento, a execução e os relatórios de manutenção.

# MP - Proteção de Mídia

## MP-1: Política e Procedimentos de Proteção de Mídia (P1)

**Descrição do Controle:**A organização:  
  
a. Desenvolve, documenta e divulga para [Atribuição: pessoal ou funções definidas pela organização]:  
  
1. Uma política de proteção à mídia que atenda a finalidade, escopo, funções, responsabilidades, compromisso de gerenciamento, coordenação entre entidades organizacionais e conformidade; e  
  
2. Procedimentos para facilitar a implementação da política de proteção de mídia e dos controles de proteção de mídia associados; e  
  
b. Analisa e atualiza a atual:  
  
1. Política de proteção de mídia [Atribuição: frequência definida pela organização]; e  
  
2. Procedimentos de proteção de mídia [Atribuição: frequência definida pela organização].  
  
**Guia Adicional:**Esse controle trata do estabelecimento de políticas e procedimentos para a implementação efetiva de controles de segurança selecionados e aprimoramentos de controle na família MP. As políticas e procedimentos refletem as leis federais aplicáveis, ordens executivas, diretivas, regulamentos, políticas, normas e diretrizes. Políticas e procedimentos do programa de segurança no nível da organização podem tornar desnecessária a necessidade de políticas e procedimentos específicos do sistema. A política pode ser incluída como parte da política geral de segurança da informação para organizações ou, inversamente, pode ser representada por múltiplas políticas refletindo a natureza complexa de certas organizações. Os procedimentos podem ser estabelecidos para o programa de segurança em geral e para sistemas de informação específicos, se necessário. A estratégia de gerenciamento de risco organizacional é um fator chave no estabelecimento de políticas e procedimentos.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-12 | https://csrc.nist.gov/publications/search?keywords-lg=800-12 |
| Publicação Especial NIST 800-100 | https://csrc.nist.gov/publications/search?keywords-lg=800-100 |

## MP-2: Acesso à Mídia (P1)

**Descrição do Controle:**A organização restringe o acesso a [Atribuição: tipos definidos por organização de mídia digital e/ou não digital] a [Atribuição: pessoal ou funções definidos pela organização].  
  
**Guia Adicional:**A mídia do sistema de informação inclui mídia digital e não digital. A mídia digital inclui, por exemplo, disquetes, fitas magnéticas, unidades de disco rígido externas / removíveis, unidades flash, discos compactos e discos de vídeo digital. Mídia não digital inclui, por exemplo, papel e microfilme. Restringir o acesso à mídia não digital inclui, por exemplo, negar o acesso aos registros médicos dos pacientes em um hospital comunitário, a menos que os indivíduos que procuram acessar esses registros sejam prestadores de serviços de saúde autorizados. Restringir o acesso à mídia digital inclui, por exemplo, limitar o acesso às especificações de design armazenadas em discos compactos na biblioteca de mídia ao líder do projeto e aos indivíduos da equipe de desenvolvimento.  
  
**Melhorias do Controle:**

### MP-2(1): Acesso à Mídia | Acesso Restrito Automatizado

[Retirado: Incorporado ao MP-4 (2)].

### MP-2(2): Acesso à Mídia | Proteção Criptográfica

[Retirado: Incorporado no SC-28 (1)].

**Referências:**

|  |  |
| --- | --- |
| Publicações de Normas Federais de Processamento de Informações N.199 | http://csrc.nist.gov/publications/PubsFIPS.html#199 |
| Publicação Especial NIST 800-111 | https://csrc.nist.gov/publications/search?keywords-lg=800-111 |

## MP-3: Marcação de Mídia (P2)

**Descrição do Controle:**A organização:  
  
a. Marca mídia do sistema de informação indicando as limitações de distribuição, tratamento de advertências e marcas de segurança aplicáveis (se houver) das informações; e  
  
b. Isenta [Atribuição: tipos de mídia do sistema de informações definidos pela organização], desde que a mídia permaneça dentro de [Atribuição: áreas controladas definidas pela organização].  
  
**Guia Adicional:**O termo marcação de segurança refere-se ao aplicativo / uso de atributos de segurança legíveis por humanos. O termo rotulagem de segurança refere-se à aplicação / uso de atributos de segurança com relação às estruturas de dados internas nos sistemas de informação (consulte AC-16). A mídia do sistema de informação inclui mídia digital e não digital. A mídia digital inclui, por exemplo, disquetes, fitas magnéticas, unidades de disco rígido externas / removíveis, unidades flash, discos compactos e discos de vídeo digital. Mídia não digital inclui, por exemplo, papel e microfilme. Geralmente, a marcação de segurança não é necessária para a mídia que contém informações determinadas pelas organizações como de domínio público ou publicamente liberáveis. No entanto, algumas organizações podem exigir marcações para informações públicas, indicando que as informações são publicamente liberáveis. A marcação da mídia do sistema de informação reflete as leis federais aplicáveis, ordens executivas, diretrizes, políticas, regulamentos, normas e orientações.

**Referências:**

|  |  |
| --- | --- |
| Publicações de Normas Federais de Processamento de Informações N.199 | http://csrc.nist.gov/publications/PubsFIPS.html#199 |

## MP-4: Armazenamento de Mídia (P1)

**Descrição do Controle:**A organização:  
  
a. Controla fisicamente e armazena com segurança [Atribuição: tipos definidos de organização de mídia digital e/ou não digital] dentro de [Atribuição: áreas controladas definidas pela organização]; e  
  
b. Protege a mídia do sistema de informações até que a mídia seja destruída ou higienizada usando equipamentos, técnicas e procedimentos aprovados.  
  
**Guia Adicional:**A mídia do sistema de informação inclui mídia digital e não digital. A mídia digital inclui, por exemplo, disquetes, fitas magnéticas, unidades de disco rígido externas / removíveis, unidades flash, discos compactos e discos de vídeo digital. Mídia não digital inclui, por exemplo, papel e microfilme. Controlar fisicamente a mídia do sistema de informações inclui, por exemplo, a realização de inventários, a garantia de procedimentos para permitir que os indivíduos façam check-out e devolva a mídia à biblioteca de mídia e a manutenção da responsabilidade por todas as mídias armazenadas. O armazenamento seguro inclui, por exemplo, uma gaveta, uma mesa ou um armário trancado ou uma biblioteca de mídia controlada. O tipo de armazenamento de mídia é proporcional à categoria de segurança e/ou classificação das informações que residem na mídia. Áreas controladas são áreas para as quais as organizações fornecem salvaguardas físicas e processuais suficientes para atender aos requisitos estabelecidos para a proteção de informações e/ou sistemas de informação. Para mídias que contenham informações determinadas pelas organizações como de domínio público, publicamente liberáveis ou com impacto limitado ou nulo sobre organizações ou indivíduos se acessadas por pessoas que não sejam pessoas autorizadas, menos proteções podem ser necessárias. Nessas situações, os controles de acesso físico fornecem proteção adequada.  
  
**Melhorias do Controle:**

### MP-4(1): Armazenamento de Mídia | Proteção Criptográfica

[Retirado: Incorporado no SC-28 (1)].

### MP-4(2): Armazenamento de Mídia | Acesso Restrito Automatizado

A organização emprega mecanismos automatizados para restringir o acesso às áreas de armazenamento de mídia e auditar tentativas de acesso e acesso concedido.  
Guia Adicional: Mecanismos automatizados podem incluir, por exemplo, teclados nas entradas externas das áreas de armazenamento de mídia.

**Referências:**

|  |  |
| --- | --- |
| Publicações de Normas Federais de Processamento de Informações N.199 | http://csrc.nist.gov/publications/PubsFIPS.html#199 |
| Publicação Especial NIST 800-56 | https://csrc.nist.gov/publications/search?keywords-lg=800-56 |
| Publicação Especial NIST 800-57 | https://csrc.nist.gov/publications/search?keywords-lg=800-57 |
| Publicação Especial NIST 800-111 | https://csrc.nist.gov/publications/search?keywords-lg=800-111 |

## MP-5: Transporte de Mídia (P1)

**Descrição do Controle:**A organização:  
  
a. Protege e controla [Atribuição: tipos de mídia do sistema de informações definidos pela organização] durante o transporte fora de áreas controladas usando [Atribuição: salvaguardas de segurança definidas pela organização];  
  
b. Mantém a responsabilidade pela mídia do sistema de informações durante o transporte fora de áreas controladas;  
  
c. Documenta as atividades associadas ao transporte da mídia do sistema de informação; e  
  
d. Restringe as atividades associadas ao transporte da mídia do sistema de informações para o pessoal autorizado.  
  
**Guia Adicional:**A mídia do sistema de informação inclui mídia digital e não digital. A mídia digital inclui, por exemplo, disquetes, fitas magnéticas, unidades de disco rígido externas / removíveis, unidades flash, discos compactos e discos de vídeo digital. Mídia não digital inclui, por exemplo, papel e microfilme. Esse controle também se aplica a dispositivos móveis com capacidade de armazenamento de informações (por exemplo, smartphones, tablets, leitores eletrônicos), que são transportados para fora de áreas controladas. Áreas controladas são áreas ou espaços para os quais as organizações fornecem salvaguardas físicas e/ou processuais suficientes para atender aos requisitos estabelecidos para a proteção de informações e/ou sistemas de informação. As salvaguardas físicas e técnicas da mídia são proporcionais à categoria ou classificação de segurança das informações que residem na mídia. As salvaguardas para proteger a mídia durante o transporte incluem, por exemplo, contêineres trancados e criptografia. Os mecanismos criptográficos podem fornecer proteções de confidencialidade e integridade, dependendo dos mecanismos utilizados. As atividades associadas ao transporte incluem o transporte real e atividades como liberar mídia para transporte e garantir que a mídia entre nos processos de transporte apropriados. Para o transporte real, o pessoal autorizado de transporte e courier pode incluir pessoas de fora da organização (por exemplo, Serviço Postal dos EUA ou um serviço de transporte ou entrega comercial). Manter a responsabilidade da mídia durante o transporte inclui, por exemplo, restringir as atividades de transporte ao pessoal autorizado e rastrear e/ou obter registros explícitos das atividades de transporte à medida que a mídia se move pelo sistema de transporte para impedir e detectar perdas, destruição ou adulteração. As organizações estabelecem requisitos de documentação para atividades associadas ao transporte de mídia do sistema de informações, de acordo com avaliações organizacionais de risco, para incluir a flexibilidade de definir diferentes métodos de manutenção de registros para os diferentes tipos de transporte de mídia como parte de um sistema geral de registros relacionados ao transporte .  
  
**Melhorias do Controle:**

### MP-5(1): Transporte de Mídia | Proteção Fora de Zonas Controladas

[Retirado: Incorporado ao MP-5].

### MP-5(2): Transporte de Mídia | Documentação de Atividades

[Retirado: Incorporado ao MP-5].

### MP-5(3): Transporte de Mídia | Custodiantes

A organização emprega um custodiante identificado durante o transporte da mídia do sistema de informações fora das áreas controladas.  
Guia Adicional: Os custodiantes identificados fornecem às organizações pontos de contato específicos durante o processo de transporte de mídia e facilitam a responsabilidade individual. As responsabilidades de custódia podem ser transferidas de um indivíduo para outro, desde que um custodiante inequívoco seja identificado o tempo todo.

### MP-5(4): Transporte de Mídia | Proteção Criptográfica

O sistema de informação implementa mecanismos criptográficos para proteger a confidencialidade e a integridade das informações armazenadas na mídia digital durante o transporte fora de áreas controladas.  
Guia Adicional: Esse aprimoramento de controle se aplica a dispositivos de armazenamento portáteis (por exemplo, cartões de memória USB, discos compactos, discos de vídeo digital, unidades de disco rígido externas / removíveis) e dispositivos móveis com capacidade de armazenamento (por exemplo, smartphones, tablets, leitores eletrônicos).

**Referências:**

|  |  |
| --- | --- |
| Publicações de Normas Federais de Processamento de Informações N.199 | http://csrc.nist.gov/publications/PubsFIPS.html#199 |
| Publicação Especial NIST 800-60 | https://csrc.nist.gov/publications/search?keywords-lg=800-60 |

## MP-6: Sanitização de Mídia (P1)

**Descrição do Controle:**A organização:  
  
a. Sanitiza [Atribuição: mídia do sistema de informações definidas pela organização] antes do descarte, liberação do controle organizacional ou liberação para reutilização usando [Atribuição: técnicas e procedimentos de sanitização definidos pela organização] de acordo com os padrões e políticas federais e organizacionais aplicáveis; e  
  
b. Emprega mecanismos de higienização com força e integridade proporcionais à categoria ou classificação de segurança das informações.  
  
**Guia Adicional:**Esse controle se aplica a todas as mídias do sistema de informação, digitais e não digitais, sujeitas a descarte ou reutilização, independentemente de a mídia ser considerada removível. Exemplos incluem mídia encontrada em scanners, copiadoras, impressoras, notebooks, estações de trabalho, componentes de rede e dispositivos móveis. O processo de higienização remove as informações da mídia, de modo que as informações não possam ser recuperadas ou reconstruídas. As técnicas de higienização, incluindo limpeza, purga, apagamento criptográfico e destruição, impedem a divulgação de informações a indivíduos não autorizados quando a mídia é reutilizada ou liberada para descarte. As organizações determinam os métodos apropriados de higienização, reconhecendo que a destruição às vezes é necessária quando outros métodos não podem ser aplicados à mídia que requer higienização. As organizações usam o critério de empregar técnicas e procedimentos aprovados de higienização para mídias que contenham informações consideradas de domínio público ou publicamente liberáveis, ou consideradas como não tendo impacto adverso em organizações ou indivíduos se liberadas para reutilização ou descarte. A higienização de mídias não digitais inclui, por exemplo, a remoção de um apêndice classificado de um documento não classificado de outra forma ou a redação de seções ou palavras selecionadas de um documento, ocultando as seções / palavras redigidas de maneira equivalente em eficácia à remoção do documento. Os padrões e políticas da NSA controlam o processo de higienização de mídias que contêm informações classificadas.  
  
**Melhorias do Controle:**

### MP-6(1): Sanitização de Mídia | Revisão / Aprovação / Trilha / Documento / Verificação

A organização revisa, aprova, rastreia, documenta e verifica as ações de higienização e descarte de mídia.  
Guia Adicional: As organizações revisam e aprovam a mídia a ser higienizada para garantir a conformidade com as políticas de retenção de registros. As ações de rastreamento / documentação incluem, por exemplo, a lista de pessoal que revisou e aprovou ações de higienização e descarte, tipos de mídia higienizados, arquivos específicos armazenados na mídia, métodos de higienização utilizados, data e hora das ações de higienização, pessoal que realizou a higienização, ações de verificação realizadas, pessoal que realizou a verificação e ações de descarte realizadas. As organizações verificam se a higienização da mídia era eficaz antes do descarte.

### MP-6(2): Sanitização de Mídia | Teste de Equipamentos

A organização testa equipamentos e procedimentos de higienização [Atribuição: frequência definida pela organização] para verificar se a higienização pretendida está sendo alcançada.  
Guia Adicional: O teste dos equipamentos e procedimentos de higienização pode ser realizado por entidades externas qualificadas e autorizadas (por exemplo, outras agências federais ou prestadores de serviços externos).

### MP-6(3): Sanitização de Mídia | Técnicas Não Destrutivas

A organização aplica técnicas de desinfecção não destrutiva a dispositivos de armazenamento portáteis antes de conectar esses dispositivos ao sistema de informações nas seguintes circunstâncias: [Atribuição: circunstâncias definidas pela organização que requerem higienização de dispositivos de armazenamento portáteis].  
Guia Adicional: Esse aprimoramento de controle se aplica a mídias digitais que contêm informações classificadas e informações não classificadas controladas (CUI). Os dispositivos de armazenamento portáteis podem ser a fonte de inserções de códigos maliciosos nos sistemas de informações organizacionais. Muitos desses dispositivos são obtidos de fontes desconhecidas e potencialmente não confiáveis e podem conter código malicioso que pode ser facilmente transferido para os sistemas de informação através de portas USB ou outros portais de entrada. Embora a verificação desses dispositivos de armazenamento seja sempre recomendada, a higienização fornece garantia adicional de que os dispositivos estão livres de código malicioso para incluir código capaz de iniciar ataques de dia zero. As organizações consideram a higienização não destrutiva de dispositivos de armazenamento portáteis quando esses dispositivos são comprados pelo fabricante ou fornecedor pela primeira vez antes do uso inicial ou quando as organizações perdem uma cadeia de custódia positiva para os dispositivos.

### MP-6(4): Sanitização de Mídia | Informação Não Classificada Controlada

[Retirado: Incorporado ao MP-6].

### MP-6(5): Sanitização de Mídia | Informação Classificada

[Retirado: Incorporado ao MP-6].

### MP-6(6): Sanitização de Mídia | Destruição de Mídia

[Retirado: Incorporado ao MP-6].

### MP-6(7): Sanitização de Mídia | Autorização Dupla

A organização impõe uma autorização dupla para a limpeza de [Atribuição: mídia do sistema de informações definido pela organização].  
Guia Adicional: As organizações empregam autorização dupla para garantir que a higienização da mídia do sistema de informações não ocorra a menos que dois indivíduos tecnicamente qualificados realizem a tarefa. Os indivíduos que higienizam a mídia do sistema de informações possuem habilidades / conhecimentos suficientes para determinar se a higienização proposta reflete os padrões, políticas e procedimentos federais / organizacionais aplicáveis. A autorização dupla também ajuda a garantir que a higienização ocorra conforme o planejado, protegendo contra erros e alegações falsas de execução das ações de higienização. A autorização dupla também pode ser conhecida como controle de duas pessoas.

### MP-6(8): Sanitização de Mídia | Remoção / Limpeza de Informação

A organização fornece a capacidade de limpar / limpar informações de [Atribuição: sistemas de informação definidos pela organização, componentes do sistema ou dispositivos] remotamente ou nas seguintes condições: [Atribuição: condições definidas pela organização].  
Guia Adicional: Esse aprimoramento de controle protege dados / informações em sistemas de informações organizacionais, componentes de sistema ou dispositivos (por exemplo, dispositivos móveis) se esses sistemas, componentes ou dispositivos forem obtidos por indivíduos não autorizados. Os comandos de limpeza / limpeza remotos requerem autenticação forte para atenuar o risco de indivíduos não autorizados limparem / limparem o sistema / componente / dispositivo. A função de limpeza / limpeza pode ser implementada de várias maneiras, incluindo, por exemplo, substituindo dados / informações várias vezes ou destruindo a chave necessária para descriptografar dados criptografados.

**Referências:**

|  |  |
| --- | --- |
| Publicações de Normas Federais de Processamento de Informações N.199 | http://csrc.nist.gov/publications/PubsFIPS.html#199 |
| Publicação Especial NIST 800-60 | https://csrc.nist.gov/publications/search?keywords-lg=800-60 |
| Publicação Especial NIST 800-88 | https://csrc.nist.gov/publications/search?keywords-lg=800-88 |
| NSA - Guia de Destruição de Mídia | http://www.nsa.gov/ia/mitigation\_guidance/media\_destruction\_guidance/index.shtml |

## MP-7: Uso de Mídia (P1)

**Descrição do Controle:**A organização [Seleção: restringe; proíbe] o uso de [Atribuição: tipos de mídia de sistema de informações definidos pela organização] em [Atribuição: sistemas de informações definidas pela organização ou componentes do sistema] usando [Atribuição: proteções de segurança definidas pela organização].  
  
**Guia Adicional:**A mídia do sistema de informação inclui mídia digital e não digital. A mídia digital inclui, por exemplo, disquetes, fitas magnéticas, unidades de disco rígido externas / removíveis, unidades flash, discos compactos e discos de vídeo digital. Mídia não digital inclui, por exemplo, papel e microfilme. Esse controle também se aplica a dispositivos móveis com capacidade de armazenamento de informações (por exemplo, smartphones, tablets, leitores eletrônicos). Ao contrário do MP-2, que restringe o acesso do usuário à mídia, esse controle restringe o uso de certos tipos de mídia nos sistemas de informação, por exemplo, restringindo / proibindo o uso de unidades flash ou unidades de disco rígido externas. As organizações podem empregar salvaguardas técnicas e não técnicas (por exemplo, políticas, procedimentos, regras de comportamento) para restringir o uso da mídia do sistema de informação. As organizações podem restringir o uso de dispositivos de armazenamento portáteis, por exemplo, usando gaiolas físicas em estações de trabalho para proibir o acesso a determinadas portas externas ou desativando / removendo a capacidade de inserir, ler ou gravar em tais dispositivos. As organizações também podem limitar o uso de dispositivos de armazenamento portáteis apenas a dispositivos aprovados, incluindo, por exemplo, dispositivos fornecidos pela organização, dispositivos fornecidos por outras organizações aprovadas e dispositivos que não são de propriedade pessoal. Finalmente, as organizações podem restringir o uso de dispositivos de armazenamento portáteis com base no tipo de dispositivo, por exemplo, proibindo o uso de dispositivos de armazenamento portáteis graváveis e implementando essa restrição desativando ou removendo a capacidade de gravar nesses dispositivos.  
  
**Melhorias do Controle:**

### MP-7(1): Uso de Mídia | Proibir o Uso Sem Proprietário

A organização proíbe o uso de dispositivos de armazenamento portáteis em sistemas de informações organizacionais quando esses dispositivos não têm proprietário identificável.  
Guia Adicional: A exigência de proprietários identificáveis (por exemplo, indivíduos, organizações ou projetos) para dispositivos de armazenamento portáteis reduz o risco de usar essas tecnologias, permitindo que as organizações atribuam responsabilidade e prestação de contas pelo tratamento de vulnerabilidades conhecidas nos dispositivos (por exemplo, inserção de código malicioso).

### MP-7(2): Uso de Mídia | Proibir o Uso de Meios Resistentes à Sanitização

A organização proíbe o uso de mídias resistentes à higienização em sistemas de informações organizacionais.  
Guia Adicional: A resistência à sanitização se aplica à capacidade de limpar informações da mídia. Certos tipos de mídia não suportam comandos de higienização ou, se suportadas, as interfaces não são suportadas de maneira padronizada nesses dispositivos. A mídia resistente à higienização inclui, por exemplo, flash compacto, flash incorporado em placas e dispositivos, unidades de estado sólido e mídia removível USB.

**Referências:**

|  |  |
| --- | --- |
| Publicações de Normas Federais de Processamento de Informações N.199 | http://csrc.nist.gov/publications/PubsFIPS.html#199 |
| Publicação Especial NIST 800-111 | https://csrc.nist.gov/publications/search?keywords-lg=800-111 |

## MP-8: Descarte de Mídia (P0)

**Descrição do Controle:**A organização:  
  
a. Estabelece [Atribuição: processo de descarte de mídia do sistema de informações definido pela organização] que inclui o emprego de mecanismos de descarte com [Atribuição: força e integridade definidas pela organização];  
  
b. Garante que o processo de descarte da mídia do sistema de informações seja proporcional à categoria de segurança e/ou ao nível de classificação das informações a serem removidas e às autorizações de acesso dos possíveis destinatários das informações desatualizadas;  
  
c. Identifica [Atribuição: mídia do sistema de informações definida pela organização que requer descarte]; e  
  
d. Descarta a mídia do sistema de informações identificado usando o processo estabelecido.  
  
**Guia Adicional:**Esse controle se aplica a todas as mídias do sistema de informação, digitais e não digitais, sujeitas a liberação fora da organização, independentemente de a mídia ser considerada removível. O processo de descarte, quando aplicado à mídia do sistema, remove as informações da mídia, geralmente por categoria de segurança ou nível de classificação, de modo que as informações não possam ser recuperadas ou reconstruídas. O descarte da mídia inclui a redação de informações para permitir uma liberação e distribuição mais amplas. O descarte da mídia também garante que o espaço vazio na mídia (por exemplo, espaço livre nos arquivos) seja desprovido de informações.  
  
**Melhorias do Controle:**

### MP-8(1): Descarte de Mídia | Documentação de Processos

A organização documenta ações de downgrade da mídia do sistema de informações.  
Guia Adicional: As organizações podem documentar o processo de desclassificação de mídia, fornecendo informações como a técnica de desclassificação empregada, o número de identificação da mídia desclassificada e a identidade da pessoa que autorizou e/ou executou a ação de desclassificação.

### MP-8(2): Descarte de Mídia | Teste de Equipamentos

A organização emprega [Atribuição: testes definidos pela organização] de equipamentos e procedimentos de desclassificação para verificar o desempenho correto [Atribuição: frequência definida pela organização].

### MP-8(3): Descarte de Mídia | Informação Não Classificada Controlada

A organização rebaixa a mídia do sistema de informações que contém [Tarefa: Informações Não Classificadas Controladas (CUI) definidas pela organização)] antes da liberação pública, de acordo com os padrões e políticas federais e organizacionais aplicáveis.

### MP-8(4): Descarte de Mídia | Informação Classificada

A organização rebaixa a mídia do sistema de informações que contém informações classificadas antes da liberação para indivíduos sem autorizações de acesso necessárias, de acordo com as normas e políticas da NSA.  
Guia Adicional: A desclassificação de informações classificadas utiliza ferramentas, técnicas e procedimentos aprovados de higienização para transferir as informações confirmadas como não classificadas dos sistemas de informação classificada para a mídia não classificada.

# PS - Segurança Pessoal

## PS-1: Política e Procedimentos de Segurança dos Funcionários (P1)

**Descrição do Controle:**A organização:  
  
a. Desenvolve, documenta e divulga para [Atribuição: pessoal ou funções definidas pela organização]:  
  
1. Uma política de segurança de pessoal que aborda finalidade, escopo, funções, responsabilidades, comprometimento gerencial, coordenação entre entidades organizacionais e conformidade; e  
  
2. Procedimentos para facilitar a implementação da política de segurança de pessoal e controles de segurança de pessoal associados; e  
  
b. Analisa e atualiza a atual:  
  
1. Política de segurança de pessoal [Atribuição: frequência definida pela organização]; e  
  
2. Procedimentos de segurança de pessoal [Atribuição: frequência definida pela organização].  
  
**Guia Adicional:**Esse controle aborda o estabelecimento de políticas e procedimentos para a implementação efetiva de controles de segurança selecionados e aprimoramentos de controle na família PS. As políticas e procedimentos refletem as leis federais aplicáveis, ordens executivas, diretivas, regulamentos, políticas, normas e diretrizes. Políticas e procedimentos do programa de segurança no nível da organização podem tornar desnecessária a necessidade de políticas e procedimentos específicos do sistema. A política pode ser incluída como parte da política geral de segurança da informação para organizações ou, inversamente, pode ser representada por múltiplas políticas refletindo a natureza complexa de certas organizações. Os procedimentos podem ser estabelecidos para o programa de segurança em geral e para sistemas de informação específicos, se necessário. A estratégia de gerenciamento de risco organizacional é um fator chave no estabelecimento de políticas e procedimentos.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-12 | https://csrc.nist.gov/publications/search?keywords-lg=800-12 |
| Publicação Especial NIST 800-100 | https://csrc.nist.gov/publications/search?keywords-lg=800-100 |

## PS-2: Designação de Riscos de Cargo (P1)

**Descrição do Controle:**A organização:  
  
a. Atribui uma designação de risco a todas as posições organizacionais;  
  
b. Estabelece critérios de triagem para os indivíduos que preencherem esses cargos; e  
  
c. Revisa e atualiza as designações de risco de posição [Atribuição: frequência definida pela organização].  
  
**Guia Adicional:**As designações de risco de posição refletem a política e a orientação do Office of Personnel Management. As designações de risco podem orientar e informar os tipos de autorizações que as pessoas recebem ao acessar informações organizacionais e sistemas de informação. Os critérios de seleção de posição incluem requisitos explícitos de nomeação de funções de segurança da informação (por exemplo, treinamento, autorizações de segurança).

**Referências:**

|  |  |
| --- | --- |
| Código de Regulamentos Federais - 5 CFR 731.106 | https://www.govinfo.gov/app/details/CFR-2012-title5-vol2/CFR-2012-title5-vol2-sec731-106 |

## PS-3: Entrevista de Funcionários (P1)

**Descrição do Controle:**A organização:  
  
a. Entrevista os indivíduos antes de autorizar o acesso ao sistema de informação; e  
  
b. Entrevista novamente as pessoas de acordo com [Tarefa: condições definidas pela organização que exigem nova triagem e, onde a nova triagem é indicada, a frequência dessa nova triagem].  
  
**Guia Adicional:**As atividades de triagem e triagem de pessoal refletem as leis federais aplicáveis, ordens executivas, diretrizes, regulamentos, políticas, normas, diretrizes e critérios específicos estabelecidos para a designação de risco dos cargos designados. As organizações podem definir diferentes condições e frequências de retransmissão para o pessoal que acessa sistemas de informação com base nos tipos de informações processadas, armazenadas ou transmitidas pelos sistemas.  
  
**Melhorias do Controle:**

### PS-3(1): Entrevista de Funcionários | Informação Classificada

A organização garante que os indivíduos que acessam um sistema de informações que processam, armazenam ou transmitem informações classificadas sejam limpos e doutrinados no nível mais alto de classificação das informações às quais têm acesso no sistema.

### PS-3(2): Entrevista de Funcionários | Doutrinação Formal

A organização garante que os indivíduos que acessam um sistema de informações que processam, armazenam ou transmitem tipos de informações classificadas que requerem doutrinação formal sejam doutrinados formalmente para todos os tipos de informações relevantes aos quais têm acesso no sistema.  
Guia Adicional: Os tipos de informações classificadas que requerem doutrinação formal incluem, por exemplo, Programa de Acesso Especial (SAP), Dados Restritos (RD) e Informações Compartimentos Sensíveis (SCI).

### PS-3(3): Entrevista de Funcionários | Informação com Medidas Especiais de Proteção

A organização garante que os indivíduos que acessam um sistema de informações processem, armazenem ou transmitam informações que exijam proteção especial:  
  
a. Ter autorizações de acesso válidas, demonstradas pelas atribuições oficiais do governo; e  
  
b. Satisfazer [Tarefa: critérios de triagem de pessoal adicional definidos pela organização].  
Guia Adicional: As informações organizacionais que exigem proteção especial incluem, por exemplo, Informações Não Classificadas Controladas (CUI) e Informações sobre Fontes e Métodos (SAMI). Os critérios de segurança do pessoal incluem, por exemplo, requisitos de triagem de histórico de sensibilidade à posição.

**Referências:**

|  |  |
| --- | --- |
| Código de Regulamentos Federais - 5 CFR 731.106 | https://www.govinfo.gov/app/details/CFR-2012-title5-vol2/CFR-2012-title5-vol2-sec731-106 |
| Publicações de Normas Federais de Processamento de Informações N.199 | http://csrc.nist.gov/publications/PubsFIPS.html#199 |
| Publicações de Normas Federais de Processamento de Informações N.201 | http://csrc.nist.gov/publications/PubsFIPS.html#201 |
| Publicação Especial NIST 800-60 | https://csrc.nist.gov/publications/search?keywords-lg=800-60 |
| Publicação Especial NIST 800-73 | https://csrc.nist.gov/publications/search?keywords-lg=800-73 |
| Publicação Especial NIST 800-76 | https://csrc.nist.gov/publications/search?keywords-lg=800-76 |
| Publicação Especial NIST 800-78 | https://csrc.nist.gov/publications/search?keywords-lg=800-78 |
| ICD 704 | https://www.dni.gov/files/documents/ICD/ICD\_704.pdf |

## PS-4: Desligamento de Funcionários (P1)

**Descrição do Controle:**A organização, após o término do emprego individual:  
  
a. Desativa o acesso ao sistema de informações dentro de [Atribuição: período definido pela organização];  
  
b. Encerra / revoga quaisquer autenticadores / credenciais associados ao indivíduo;  
  
c. Realiza entrevistas de saída que incluem uma discussão sobre [Tarefa: tópicos de segurança da informação definidos pela organização];  
  
d. Recupera toda a propriedade relacionada ao sistema de informações organizacionais relacionadas à segurança;  
  
e. Mantém o acesso às informações organizacionais e sistemas de informação anteriormente controlados por indivíduos demitidos; e  
  
f. Notifica [Atribuição: pessoal ou funções definidas pela organização] dentro de [Atribuição: período definido pela organização].  
  
**Guia Adicional:**As propriedades relacionadas ao sistema de informações incluem, por exemplo, tokens de autenticação de hardware, manuais técnicos de administração do sistema, chaves, cartões de identificação e passes de construção. As entrevistas de saída garantem que os indivíduos demitidos compreendam as restrições de segurança impostas por serem ex-funcionários e que a responsabilidade adequada seja alcançada pelas propriedades relacionadas ao sistema de informações. Os tópicos de segurança de interesse nas entrevistas de saída podem incluir, por exemplo, lembrar indivíduos rescindidos de acordos de confidencialidade e possíveis limitações em empregos futuros. As entrevistas de saída podem não ser possíveis para alguns indivíduos demitidos, por exemplo, em casos relacionados a abandono de emprego, doenças e indisponibilidade de supervisores. As entrevistas de saída são importantes para indivíduos com folgas de segurança. A execução oportuna de ações de rescisão é essencial para indivíduos rescindidos por justa causa. Em certas situações, as organizações consideram desabilitar as contas do sistema de informações de indivíduos que estão sendo finalizados antes de os indivíduos serem notificados.  
  
**Melhorias do Controle:**

### PS-4(1): Desligamento de Funcionários | Requisitos Pós-Contratação

A organização:  
  
a. Notifica indivíduos demitidos de requisitos pós-contratação, juridicamente vinculativos aplicáveis para a proteção de informações organizacionais; e  
  
b. Requer que as pessoas demitidas assinem uma confirmação de requisitos pós-contratação como parte do processo de rescisão organizacional.  
Guia Adicional: As organizações consultam o Gabinete do Conselho Geral sobre questões de requisitos pós-contratação para indivíduos demitidos.

### PS-4(2): Desligamento de Funcionários | Notificação Automatizada

A organização emprega mecanismos automatizados para notificar [Atribuição: pessoal ou funções definidas pela organização] após a rescisão de um indivíduo.  
Guia Adicional: Nas organizações com um grande número de funcionários, nem todo pessoal que precisa conhecer as ações de rescisão recebe as notificações apropriadas - ou, se essas notificações forem recebidas, elas podem não ocorrer em tempo hábil. Mecanismos automatizados podem ser usados para enviar alertas ou notificações automáticas para funções ou pessoal organizacional específico (por exemplo, pessoal de gerência, supervisores, agentes de segurança pessoal, agentes de segurança da informação, administradores de sistemas ou administradores de tecnologia da informação) quando indivíduos são demitidos. Esses alertas ou notificações automáticos podem ser transmitidos de várias maneiras, incluindo, por exemplo, por telefone, via correio eletrônico, mensagem de texto ou sites.

## PS-5: Transferência de Funcionários (P2)

**Descrição do Controle:**A organização:  
  
a. Analisa e confirma a necessidade operacional contínua de autorizações atuais de acesso lógico e físico a sistemas / instalações de informação quando indivíduos são transferidos ou transferidos para outras posições dentro da organização;  
  
b. Inicia [Cessão: ações de transferência ou transferência definida pela organização] dentro de [Cessão: período definido pela organização após a ação formal de transferência];  
  
c. Modifica a autorização de acesso conforme necessário para corresponder a quaisquer mudanças na necessidade operacional devido à reatribuição ou transferência; e  
  
d. Notifica [Atribuição: pessoal ou funções definidas pela organização] dentro de [Atribuição: período definido pela organização].  
  
**Guia Adicional:**Esse controle se aplica quando as reatribuições ou transferências de indivíduos são permanentes ou com durações prolongadas que tornam as ações justificadas. As organizações definem ações apropriadas para os tipos de reatribuições ou transferências, permanentes ou estendidas. As ações que podem ser necessárias para transferências ou transferências de pessoal para outros cargos nas organizações incluem, por exemplo: (i) devolução antiga e emissão de novas chaves, cartões de identificação e passes de construção; (ii) fechamento de contas do sistema de informação e estabelecimento de novas contas; (iii) alteração das autorizações de acesso ao sistema de informação (ou seja, privilégios); e (iv) fornecer acesso a registros oficiais aos quais os indivíduos tiveram acesso em locais de trabalho anteriores e em contas anteriores do sistema de informação.

## PS-6: Acordos de Acesso (P3)

**Descrição do Controle:**A organização:  
  
a. Desenvolve e documenta acordos de acesso para sistemas de informação organizacional;  
  
b. Revisa e atualiza os contratos de acesso [Atribuição: frequência definida pela organização]; e  
  
c. Garante que os indivíduos que precisam acessar informações organizacionais e sistemas de informação:  
  
1. Assine contratos de acesso apropriados antes de receber acesso; e  
  
2. Revalide a assinatura dos contratos de acesso para manter o acesso aos sistemas de informações organizacionais quando os contratos de acesso forem atualizados ou [Atribuição: frequência definida pela organização].  
  
**Guia Adicional:**Os contratos de acesso incluem, por exemplo, contratos de confidencialidade, contratos de uso aceitável, regras de comportamento e acordos de conflito de interesses. Os contratos de acesso assinados incluem um reconhecimento de que os indivíduos leram, entenderam e concordam em cumprir as restrições associadas aos sistemas de informações organizacionais para os quais o acesso é autorizado. As organizações podem usar assinaturas eletrônicas para reconhecer contratos de acesso, a menos que especificamente proibido pela política organizacional.  
  
**Melhorias do Controle:**

### PS-6(1): Acordos de Acesso | Informação que Exige Proteção Especial

[Retirado: Incorporado ao PS-3].

### PS-6(2): Acordos de Acesso | Informação Classificada que Exige Proteção Especial

A organização garante que o acesso a informações classificadas que exijam proteção especial seja concedido apenas a indivíduos que:  
  
a. Ter uma autorização de acesso válida, demonstrada pelas atribuições oficiais do governo;  
  
b. Satisfazer os critérios de segurança do pessoal associado; e  
  
c. Leu, entendeu e assinou um contrato de confidencialidade.  
Guia Adicional: As informações classificadas que exigem proteção especial incluem, por exemplo, informações colaterais, informações do Programa de Acesso Especial (SAP) e Informações Compartidas Sensíveis (SCI). Os critérios de segurança do pessoal refletem as leis federais aplicáveis, ordens executivas, diretrizes, regulamentos, políticas, padrões e orientações.

### PS-6(3): Acordos de Acesso | Requisitos Pós-Contratação

A organização:  
  
a. Notifica as pessoas sobre os requisitos pós-contratação, juridicamente vinculativos, aplicáveis à proteção das informações organizacionais; e  
  
b. Requer que os indivíduos assinem um reconhecimento desses requisitos, se aplicável, como parte da concessão de acesso inicial às informações cobertas.  
Guia Adicional: As organizações consultam o Gabinete do Conselho Geral sobre questões de requisitos pós-contratação para indivíduos demitidos.

## PS-7: Segurança dos Terceiros (P1)

**Descrição do Controle:**A organização:  
  
a. Estabelece requisitos de segurança de pessoal, incluindo funções e responsabilidades de segurança para fornecedores terceirizados;  
  
b. Exige que fornecedores terceirizados cumpram as políticas e procedimentos de segurança de pessoal estabelecidos pela organização;  
  
c. Documenta os requisitos de segurança do pessoal;  
  
d. Requer que fornecedores terceirizados notifiquem [Cessão: pessoal ou funções definidas pela organização] de quaisquer transferências ou demissões de pessoal de terceiros que possuam credenciais e/ou crachás organizacionais ou que tenham privilégios de sistema de informação em [Cessão: definida pela organização período de tempo]; e  
  
e. Monitora a conformidade do provedor.  
  
**Guia Adicional:**Os fornecedores de terceiros incluem, por exemplo, agências de serviços, contratados e outras organizações que fornecem desenvolvimento de sistemas de informação, serviços de tecnologia da informação, aplicativos terceirizados e gerenciamento de rede e segurança. As organizações incluem explicitamente requisitos de segurança de pessoal em documentos relacionados à aquisição. Fornecedores terceirizados podem ter pessoal trabalhando em instalações organizacionais com credenciais, crachás ou privilégios de sistema de informação emitidos por organizações. As notificações de alterações de pessoal de terceiros garantem o término apropriado de privilégios e credenciais. As organizações definem as transferências e terminações consideradas reportáveis por características relacionadas à segurança que incluem, por exemplo, funções, funções e natureza de credenciais / privilégios associados a indivíduos transferidos ou rescindidos.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-35 | https://csrc.nist.gov/publications/search?keywords-lg=800-35 |

## PS-8: Sanções dos Funcionários (P3)

**Descrição do Controle:**A organização:  
  
a. Emprega um processo formal de sanções para indivíduos que não cumprem as políticas e procedimentos estabelecidos de segurança da informação; e  
  
b. Notifica [Cessão: pessoal ou funções definidas pela organização] dentro de [Cessão: período de tempo definido pela organização] quando um processo formal de sanções a funcionários é iniciado, identificando o indivíduo sancionado e o motivo da sanção.  
  
**Guia Adicional:**Os processos de sanções organizacionais refletem as leis federais aplicáveis, ordens executivas, diretrizes, regulamentos, políticas, normas e orientações. Os processos de sanções são descritos em contratos de acesso e podem ser incluídos como parte das políticas e procedimentos gerais de pessoal para as organizações. As organizações consultam o Escritório do Conselho Geral sobre questões de sanções dos funcionários.

# PE - Proteção Física e Ambiental

## PE-1: Política e Procedimentos de Proteção Física e Ambiental (P1)

**Descrição do Controle:**A organização:  
  
a. Desenvolve, documenta e dissemina para [Atribuição: pessoal ou funções definidas pela organização]:  
  
1. Uma política de proteção física e ambiental que lide com propósito, escopo, funções, responsabilidades, compromisso de gerenciamento, coordenação entre entidades organizacionais e conformidade; e  
  
2. Procedimentos para facilitar a implementação da política de proteção física e ambiental e os controles de proteção física e ambiental associados; e  
  
b. Revisa e atualiza a atual:  
  
1. Política de proteção física e ambiental [Atribuição: frequência definida pela organização]; e  
  
2. Procedimentos de proteção física e ambiental [Atribuição: frequência definida pela organização].  
  
**Guia Adicional:**Esse controle trata do estabelecimento de políticas e procedimentos para a implementação efetiva de controles de segurança selecionados e aprimoramentos de controle na família PE. As políticas e procedimentos refletem as leis federais aplicáveis, ordens executivas, diretivas, regulamentos, políticas, normas e diretrizes. Políticas e procedimentos do programa de segurança no nível da organização podem tornar desnecessária a necessidade de políticas e procedimentos específicos do sistema. A política pode ser incluída como parte da política geral de segurança da informação para organizações ou, inversamente, pode ser representada por múltiplas políticas refletindo a natureza complexa de certas organizações. Os procedimentos podem ser estabelecidos para o programa de segurança em geral e para sistemas de informação específicos, se necessário. A estratégia de gerenciamento de risco organizacional é um fator chave no estabelecimento de políticas e procedimentos.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-12 | https://csrc.nist.gov/publications/search?keywords-lg=800-12 |
| Publicação Especial NIST 800-113 | https://csrc.nist.gov/publications/search?keywords-lg=800-113 |

## PE-2: Autorizações de Acesso Físico (P1)

**Descrição do Controle:**A organização:  
  
a. Desenvolve, aprova e mantém uma lista de indivíduos com acesso autorizado às instalações onde o sistema de informações reside;  
  
b. Emite credenciais de autorização para acesso a instalações;  
  
c. Revisa a lista de acesso que detalha o acesso autorizado às instalações por indivíduos [Tarefa: frequência definida pela organização]; e  
  
d. Remove indivíduos da lista de acesso da instalação quando o acesso não é mais necessário.  
  
**Guia Adicional:**Esse controle se aplica aos funcionários e visitantes da organização. Indivíduos (por exemplo, funcionários, contratados e outros) com credenciais permanentes de autorização de acesso físico não são considerados visitantes. As credenciais de autorização incluem, por exemplo, crachás, cartões de identificação e cartões inteligentes. As organizações determinam a força das credenciais de autorização necessárias (incluindo o nível de crachás à prova de falsificação, cartões inteligentes ou cartões de identificação) de acordo com os padrões, políticas e procedimentos federais. Este controle se aplica apenas a áreas dentro de instalações que não foram designadas como acessíveis ao público.  
  
**Melhorias do Controle:**

### PE-2(1): Autorizações de Acesso Físico | Acesso por Posição / Cargo

A organização autoriza o acesso físico às instalações onde o sistema de informações reside, com base na posição ou função.

### PE-2(2): Autorizações de Acesso Físico | Duas Formas de Identificação

A organização requer duas formas de identificação em [Tarefa: lista definida pela organização de formas aceitáveis de identificação] para acesso do visitante às instalações em que o sistema de informações reside.  
Guia Adicional: As formas aceitáveis de identificação com foto do governo incluem, por exemplo, passaportes, cartões de verificação de identidade pessoal (PIV) e carteiras de motorista. No caso de obter acesso às instalações usando mecanismos automatizados, as organizações podem usar cartões PIV, cartões-chave, PINs e biometria.

### PE-2(3): Autorizações de Acesso Físico | Acesso Restritivo Não Estratégico

A organização restringe o acesso sem escolta à instalação onde o sistema de informações reside para o pessoal com [Seleção (uma ou mais): liberações de segurança para todas as informações contidas no sistema; autorizações formais de acesso a todas as informações contidas no sistema; necessidade de acesso a todas as informações contidas no sistema; [Atribuição: credenciais definidas pela organização]].  
Guia Adicional: Devido à natureza altamente sensível das informações classificadas armazenadas em certas instalações, é importante que os indivíduos que não dispõem de autorizações de segurança suficientes, aprovações de acesso ou precisem saber sejam escoltados por indivíduos com credenciais apropriadas para garantir que essas informações não sejam expostas ou comprometidas. .

## PE-3: Controle de Acesso Físico (P1)

**Descrição do Controle:**A organização:  
  
a. Impõe autorizações de acesso físico em [Atribuição: pontos de entrada / saída definidos pela organização para a instalação em que o sistema de informações reside];  
  
1. Verificar autorizações de acesso individuais antes de conceder acesso à instalação; e  
  
2. Controlar a entrada / saída da instalação usando [Seleção (uma ou mais): [Atribuição: sistemas / dispositivos de controle de acesso físico definidos pela organização]; guardas];  
  
b. Mantém registros de auditoria de acesso físico para [Atribuição: pontos de entrada / saída definidos pela organização];  
  
c. Fornece [Atribuição: salvaguardas de segurança definidas pela organização] para controlar o acesso a áreas dentro da instalação oficialmente designadas como acessíveis ao público;  
  
d. Acompanha os visitantes e monitora a atividade dos visitantes [Tarefa: circunstâncias definidas pela organização que exigem escolta e monitoramento de visitantes];  
  
e. Protege chaves, combinações e outros dispositivos de acesso físico;  
  
f. Inventários [Cessão: dispositivos de acesso físico definidos pela organização] a cada [Cessão: frequência definida pela organização]; e  
  
g. Altera combinações e chaves [Atribuição: frequência definida pela organização] e/ou quando as chaves são perdidas, as combinações são comprometidas ou os indivíduos são transferidos ou finalizados.  
  
**Guia Adicional:**Esse controle se aplica aos funcionários e visitantes da organização. Indivíduos (por exemplo, funcionários, contratados e outros) com credenciais permanentes de autorização de acesso físico não são considerados visitantes. As organizações determinam os tipos de guardas necessários para as instalações, incluindo, por exemplo, pessoal profissional de segurança física ou outro pessoal, como pessoal administrativo ou usuários de sistemas de informação. Os dispositivos de acesso físico incluem, por exemplo, chaves, bloqueios, combinações e leitores de cartão. As salvaguardas para áreas acessíveis ao público dentro das instalações da organização incluem, por exemplo, câmeras, monitoramento por guardas e isolamento de sistemas de informações selecionados e/ou componentes de sistemas em áreas seguras. Os sistemas de controle de acesso físico estão em conformidade com as leis federais aplicáveis, ordens executivas, diretrizes, políticas, regulamentos, normas e orientações. O Programa Federal de Identidade, Credencial e Gerenciamento de Acesso fornece diretrizes de implementação para recursos de gerenciamento de identidade, credencial e acesso para sistemas de controle de acesso físico. As organizações têm flexibilidade nos tipos de logs de auditoria empregados. Os registros de auditoria podem ser procedurais (por exemplo, um registro por escrito de indivíduos acessando a instalação e quando esse acesso ocorreu), automatizados (por exemplo, capturando o ID fornecido por um cartão PIV) ou alguma combinação dos mesmos. Os pontos de acesso físico podem incluir pontos de acesso da instalação, pontos de acesso internos a sistemas de informação e/ou componentes que requerem controles de acesso suplementares, ou ambos. Os componentes dos sistemas de informações organizacionais (por exemplo, estações de trabalho, terminais) podem estar localizados em áreas designadas como acessíveis ao público com organizações que protegem o acesso a esses dispositivos.  
  
**Melhorias do Controle:**

### PE-3(1): Controle de Acesso Físico | Acesso ao Sistema de Informação

A organização aplica autorizações de acesso físico ao sistema de informações, além dos controles de acesso físico para a instalação em [Atribuição: espaços físicos definidos pela organização que contêm um ou mais componentes do sistema de informações].  
Guia Adicional: Esse aprimoramento de controle fornece segurança física adicional para as áreas dentro de instalações onde há uma concentração de componentes do sistema de informações (por exemplo, salas de servidores, áreas de armazenamento de mídia, centros de dados e comunicações).

### PE-3(2): Controle de Acesso Físico | Fronteiras do Sistema de Instalação / Informação

A organização realiza verificações de segurança [Atribuição: frequência definida pela organização] no limite físico da instalação ou sistema de informação para exfiltração não autorizada de informações ou remoção de componentes do sistema de informações.  
Guia Adicional: As organizações determinam a extensão, a frequência e/ou a aleatoriedade das verificações de segurança para mitigar adequadamente os riscos associados à exfiltração.

### PE-3(3): Controle de Acesso Físico | Guarda Contínua / Alarmes / Monitoramento

A organização emprega guardas e/ou alarmes para monitorar todos os pontos de acesso físico às instalações onde o sistema de informações reside 24 horas por dia, 7 dias por semana.

### PE-3(4): Controle de Acesso Físico | Caixas Lacráveis

A organização usa invólucros físicos bloqueáveis para proteger [Atribuição: componentes do sistema de informações definidos pela organização] contra acesso físico não autorizado.

### PE-3(5): Controle de Acesso Físico | Proteção Contra Manipulação

A organização emprega [Atribuição: salvaguardas de segurança definidas pela organização] para [Seleção (uma ou mais): detectar; impedir] adulteração física ou alteração de [Atribuição: componentes de hardware definidos pela organização] dentro do sistema de informação.  
Guia Adicional: As organizações podem implementar detecção / prevenção de violação em componentes de hardware selecionados ou detecção de violação em alguns componentes e prevenção de violação em outros componentes. As atividades de detecção / prevenção de violação podem empregar muitos tipos de tecnologias anti-violação, incluindo, por exemplo, selos de detecção de violação e revestimentos anti-violação. Os programas anti-adulteração ajudam a detectar alterações de hardware por meio de falsificação e outros riscos relacionados à cadeia de suprimentos.

### PE-3(6): Controle de Acesso Físico | Pen Test das Instalações

A organização emprega um processo de teste de penetração que inclui [Atribuição: frequência definida pela organização], tentativas não anunciadas de contornar ou contornar os controles de segurança associados aos pontos de acesso físico à instalação.

**Referências:**

|  |  |
| --- | --- |
| Publicações de Normas Federais de Processamento de Informações N.201 | http://csrc.nist.gov/publications/PubsFIPS.html#201 |
| Publicação Especial NIST 800-73 | https://csrc.nist.gov/publications/search?keywords-lg=800-73 |
| Publicação Especial NIST 800-76 | https://csrc.nist.gov/publications/search?keywords-lg=800-76 |
| Publicação Especial NIST 800-78 | https://csrc.nist.gov/publications/search?keywords-lg=800-78 |
| Publicação Especial NIST 800-116 | https://csrc.nist.gov/publications/search?keywords-lg=800-116 |
| ICD 704 | https://www.dni.gov/files/documents/ICD/ICD\_704.pdf |
| ICD 705 | https://www.dni.gov/files/documents/ICD/ICD\_705\_SCIFs.pdf |
| Instruções do Departamento de Defesa dos EUA N.5200.39 | https://www.dami.army.pentagon.mil/site/ARTPC/docs/DODI%205200\_39p.pdf |
| FICAM: Identidade Federal, Credencial e Gerenciamento de Acesso | http://idmanagement.gov |

## PE-4: Controle de Acesso para Meios de Transmissão (P1)

**Descrição do Controle:**A organização controla o acesso físico a [Atribuição: linhas de transmissão e transmissão de sistemas de informações definidas pela organização] dentro das instalações da organização usando [Atribuição: salvaguardas de segurança definidas pela organização].  
  
**Guia Adicional:**As salvaguardas de segurança física aplicadas às linhas de distribuição e transmissão do sistema de informações ajudam a evitar danos acidentais, interrupções e violações físicas. Além disso, podem ser necessárias salvaguardas físicas para ajudar a impedir a interceptação ou a modificação em trânsito de transmissões não criptografadas. As salvaguardas de segurança para controlar o acesso físico às linhas de distribuição e transmissão do sistema incluem, por exemplo: (i) armários de fiação trancados; (ii) tomadas sobressalentes desconectadas ou bloqueadas; e/ou (iii) proteção de cabos por conduítes ou bandejas de cabos.

**Referências:**

|  |  |
| --- | --- |
| CNSS - NSTISSI N.7003 | http://www.cnss.gov/Assets/pdf/nstissi\_7003.pdf |

## PE-5: Controle de Acesso para Dispositivos de Saída (P2)

**Descrição do Controle:**A organização controla o acesso físico aos dispositivos de saída do sistema de informações para impedir que indivíduos não autorizados obtenham a saída.  
  
**Guia Adicional:**O controle do acesso físico aos dispositivos de saída inclui, por exemplo, a colocação de dispositivos de saída em salas bloqueadas ou outras áreas protegidas e a permissão de acesso apenas a indivíduos autorizados e a colocação de dispositivos de saída em locais que podem ser monitorados pelo pessoal da organização. Monitores, impressoras, copiadoras, scanners, aparelhos de fac-símile e dispositivos de áudio são exemplos de dispositivos de saída do sistema de informações.  
  
**Melhorias do Controle:**

### PE-5(1): Controle de Acesso para Dispositivos de Saída | Acesso à Saída por Indivíduos Autorizados

A organização:  
  
a. Controla o acesso físico à saída de [Atribuição: dispositivos de saída definidos pela organização]; e  
  
b. Garante que apenas pessoas autorizadas recebam saída do dispositivo.  
Guia Adicional: O controle do acesso físico a dispositivos de saída selecionados inclui, por exemplo, a colocação de impressoras, copiadoras e máquinas de fax em áreas controladas com controles de acesso pelo teclado ou limitar o acesso a indivíduos com certos tipos de emblemas.

### PE-5(2): Controle de Acesso para Dispositivos de Saída | Acesso à Saída por Identidade Individual

O sistema de informação:  
  
a. Controla o acesso físico à saída de [Atribuição: dispositivos de saída definidos pela organização]; e  
  
b. Vincula a identidade individual ao recebimento da saída do dispositivo.  
Guia Adicional: O controle do acesso físico aos dispositivos de saída selecionados inclui, por exemplo, a instalação de funcionalidades de segurança em impressoras, copiadoras e máquinas de fax que permitem que as organizações implementem autenticação (por exemplo, usando um PIN ou token de hardware) nos dispositivos de saída antes da liberação da saída para indivíduos. .

### PE-5(3): Controle de Acesso para Dispositivos de Saída | Marcando Dispositivos de Saída

A organização marca [Atribuição: dispositivos de saída do sistema de informações definidos pela organização] indicando a marcação de segurança apropriada das informações que podem ser enviadas pelo dispositivo.  
Guia Adicional: Os dispositivos de saída incluem, por exemplo, impressoras, monitores, máquinas de fax, scanners, copiadoras e dispositivos de áudio. Esse aprimoramento de controle é geralmente aplicável a dispositivos de saída do sistema de informação que não sejam dispositivos móveis.

## PE-6: Monitorando o Acesso Físico (P1)

**Descrição do Controle:**A organização:  
  
a. Monitora o acesso físico às instalações onde o sistema de informações reside para detectar e responder a incidentes de segurança física;  
  
b. Revisa os logs de acesso físico [Atribuição: frequência definida pela organização] e após a ocorrência de [Atribuição: eventos definidos pela organização ou possíveis indicações de eventos]; e  
  
c. Coordena os resultados de análises e investigações com a capacidade de resposta a incidentes organizacionais.  
  
**Guia Adicional:**Os recursos organizacionais de resposta a incidentes incluem investigações e respostas a incidentes de segurança física detectados. Os incidentes de segurança incluem, por exemplo, aparentes violações de segurança ou atividades suspeitas de acesso físico. As atividades de acesso físico suspeito incluem, por exemplo: (i) acessos fora do horário normal de trabalho; (ii) acessos repetidos a áreas normalmente não acessadas; (iii) acessos por períodos incomuns; e (iv) acessos fora de sequência.  
  
**Melhorias do Controle:**

### PE-6(1): Monitorando o Acesso Físico | Alarme de Intrusão / Equipamento de Vigilância

A organização monitora alarmes de intrusão física e equipamentos de vigilância.

### PE-6(2): Monitorando o Acesso Físico | Reconhecimento Automatizado / Respostas à Intrusão

A organização emprega mecanismos automatizados para reconhecer [Tarefa: classes definidas pela organização / tipos de intrusões] e iniciar [Tarefa: ações de resposta definidas pela organização].

### PE-6(3): Monitorando o Acesso Físico | Video Vigilância

A organização emprega vigilância por vídeo de [Tarefa: áreas operacionais definidas pela organização] e retém gravações de vídeo por [Tarefa: período de tempo definido pela organização].  
Guia Adicional: Esse aprimoramento de controle concentra-se na gravação de vídeo de vigilância para fins de revisão subsequente, se as circunstâncias o justificarem (por exemplo, uma invasão detectada por outros meios). Não requer monitoramento de vídeo de vigilância, embora as organizações possam optar por fazê-lo. Observe que pode haver considerações legais ao executar e manter a vigilância por vídeo, especialmente se essa vigilância estiver em um local público.

### PE-6(4): Monitorando o Acesso Físico | Monitorando o Acesso Físico a Sistemas de Informação

A organização monitora o acesso físico ao sistema de informação, além do monitoramento do acesso físico da instalação como [Atribuição: espaços físicos definidos pela organização que contêm um ou mais componentes do sistema de informação].  
Guia Adicional: Esse aprimoramento de controle fornece monitoramento adicional para as áreas dentro de instalações onde há uma concentração de componentes do sistema de informações (por exemplo, salas de servidores, áreas de armazenamento de mídia, centros de comunicação).

## PE-7: Controle do Visitante (P0)

**Descrição do Controle:**[Retirado: Incorporado em PE-2 e PE-3].

## PE-8: Registros de Acesso ao Visitante (P3)

**Descrição do Controle:**A organização:  
  
a. Mantém registros de acesso de visitantes às instalações onde o sistema de informações reside por [Atribuição: período definido pela organização]; e  
  
b. Revisa os registros de acesso do visitante [Atribuição: frequência definida pela organização].  
  
**Guia Adicional:**Os registros de acesso de visitantes incluem, por exemplo, nomes e organizações de pessoas que visitam, assinaturas de visitantes, formas de identificação, datas de acesso, horários de entrada e saída, propósitos de visitas e nomes e organizações de pessoas visitadas. Os registros de acesso de visitantes não são necessários para áreas acessíveis ao público.  
  
**Melhorias do Controle:**

### PE-8(1): Registros de Acesso ao Visitante | Manutenção / Revisão Automática de Registros

A organização emprega mecanismos automatizados para facilitar a manutenção e a revisão dos registros de acesso dos visitantes.

### PE-8(2): Registros de Acesso ao Visitante | Registros de Acesso Físico

[Retirado: Incorporado ao PE-2].

## PE-9: Equipamentos de Energia e Cabos (P1)

**Descrição do Controle:**A organização protege o equipamento de energia e o cabeamento de energia para o sistema de informações contra danos e destruição.  
  
**Guia Adicional:**As organizações determinam os tipos de proteção necessários para equipamentos e cabos de energia empregados em diferentes locais, internos e externos às instalações organizacionais e aos ambientes de operação. Isso inclui, por exemplo, geradores e cabos de energia fora dos edifícios, cabos internos e fontes de energia ininterrupta dentro de um escritório ou data center, e fontes de energia para entidades independentes, como veículos e satélites.  
  
**Melhorias do Controle:**

### PE-9(1): Equipamentos de Energia e Cabos | Cabos Redundantes

A organização emprega caminhos de cabos de energia redundantes que são fisicamente separados por [Atribuição: distância definida pela organização].  
Guia Adicional: Os cabos de energia redundantes e fisicamente separados ajudam a garantir que a energia continue fluindo no caso de um dos cabos ser cortado ou danificado.

### PE-9(2): Equipamentos de Energia e Cabos | Controles Automáticos de Tensão

A organização emprega controles automáticos de tensão para [Atribuição: componentes do sistema de informações críticas definidas pela organização].

## PE-10: Desligamento de Emergência (P1)

**Descrição do Controle:**A organização:  
  
a. Fornece a capacidade de desligar a energia do sistema de informações ou de componentes individuais do sistema em situações de emergência;  
  
b. Coloca interruptores ou dispositivos de desligamento de emergência em [Atribuição: local definido pela organização por sistema de informação ou componente do sistema] para facilitar o acesso fácil e seguro ao pessoal; e  
  
c. Protege o recurso de desligamento de energia de emergência contra ativação não autorizada.  
  
**Guia Adicional:**Esse controle se aplica principalmente a instalações que contêm concentrações de recursos do sistema de informações, incluindo, por exemplo, centros de dados, salas de servidores e salas de computadores de mainframe.  
  
**Melhorias do Controle:**

### PE-10(1): Desligamento de Emergência | Ativação Acidental / Não Autorizada

[Retirado: Incorporado ao PE-10].

## PE-11: Energia de Emergência (P1)

**Descrição do Controle:**A organização fornece uma fonte de alimentação ininterrupta de curto prazo para facilitar [Seleção (uma ou mais): um desligamento ordenado do sistema de informação; transição do sistema de informação para energia alternativa de longo prazo] no caso de perda primária da fonte de energia.  
  
**Melhorias do Controle:**

### PE-11(1): Energia de Emergência | Alimentação Alternativa a Longo Prazo - Capacidade Operacional Mínima

A organização fornece uma fonte de alimentação alternativa de longo prazo para o sistema de informações capaz de manter a capacidade operacional minimamente exigida no caso de uma perda prolongada da fonte de energia primária.  
Guia Adicional: Esse aprimoramento de controle pode ser satisfeito, por exemplo, pelo uso de uma fonte de alimentação comercial secundária ou outra fonte de alimentação externa. As fontes de alimentação alternativas de longo prazo para o sistema de informações podem ser ativadas manual ou automaticamente.

### PE-11(2): Energia de Emergência | Fonte de Alimentação Alternativa a Longo Prazo - Automatizada

A organização fornece uma fonte de alimentação alternativa de longo prazo para o sistema de informações que é:  
  
a. Autônomo;  
  
b. Não depende de geração de energia externa; e  
  
c. Capaz de manter [Seleção: capacidade operacional minimamente exigida; capacidade operacional total] no caso de uma perda prolongada da fonte de energia primária.  
Guia Adicional: Esse aprimoramento de controle pode ser satisfeito, por exemplo, pelo uso de um ou mais geradores com capacidade suficiente para atender às necessidades da organização. Fontes de alimentação alternativas de longo prazo para sistemas de informações organizacionais são ativadas manual ou automaticamente.

## PE-12: Luz de Emergência (P1)

**Descrição do Controle:**A organização emprega e mantém iluminação de emergência automática para o sistema de informações que é ativado no caso de falta de energia ou interrupção e que cobre saídas de emergência e rotas de evacuação dentro da instalação.  
  
**Guia Adicional:**Esse controle se aplica principalmente a instalações que contêm concentrações de recursos do sistema de informações, incluindo, por exemplo, centros de dados, salas de servidores e salas de computadores de mainframe.  
  
**Melhorias do Controle:**

### PE-12(1): Luz de Emergência | Missões Essenciais / Funções de Negócio

A organização fornece iluminação de emergência para todas as áreas da instalação, apoiando missões essenciais e funções de negócios.

## PE-13: Proteção Contra Fogo (P1)

**Descrição do Controle:**A organização emprega e mantém dispositivos / sistemas de detecção e supressão de incêndio para o sistema de informação que são apoiados por uma fonte de energia independente.  
  
**Guia Adicional:**Esse controle se aplica principalmente a instalações que contêm concentrações de recursos do sistema de informações, incluindo, por exemplo, centros de dados, salas de servidores e salas de computadores de mainframe. Os dispositivos / sistemas de supressão e detecção de incêndio incluem, por exemplo, sistemas de sprinklers, extintores de incêndio portáteis, mangueiras fixas de incêndio e detectores de fumaça.  
  
**Melhorias do Controle:**

### PE-13(1): Proteção Contra Fogo | Dispositivos / Sistemas de Detecção

A organização emprega dispositivos / sistemas de detecção de incêndio para o sistema de informação que é ativado automaticamente e notifica [Atribuição: pessoal ou funções definidas pela organização] e [Atribuição: equipes de emergência definidas pela organização] em caso de incêndio.  
Guia Adicional: As organizações podem identificar pessoal, funções e equipes de atendimento a emergências específicas, caso as pessoas na lista de notificação devam ter autorizações de acesso e/ou autorizações apropriadas, por exemplo, para obter acesso às instalações onde estão ocorrendo operações classificadas ou onde existem sistemas de informação contendo informações classificadas.

### PE-13(2): Proteção Contra Fogo | Dispositivos / Sistemas de Supressão

A organização emprega dispositivos / sistemas de supressão de incêndio para o sistema de informações que fornecem notificação automática de qualquer ativação à Tarefa: pessoal ou funções definidas pela organização] e [Tarefa: equipes de emergência definidas pela organização].  
Guia Adicional: As organizações podem identificar pessoal, funções e equipes de atendimento a emergências específicas, caso as pessoas na lista de notificação devam ter autorizações de acesso e/ou autorizações apropriadas, por exemplo, para obter acesso às instalações onde estão ocorrendo operações classificadas ou onde existem sistemas de informação contendo informações classificadas.

### PE-13(3): Proteção Contra Fogo | Supressão Automática de Incêndio

A organização emprega um recurso automático de supressão de incêndio para o sistema de informações quando a instalação não possui funcionários em uma base contínua.

### PE-13(4): Proteção Contra Fogo | Inspeções

A organização assegura que a instalação seja submetida a inspeções [Atribuição: frequência definida pela organização] por inspetores autorizados e qualificados e resolva as deficiências identificadas dentro de [Atribuição: período definido pela organização].

## PE-14: Controles de Temperatura e Umidade (P1)

**Descrição do Controle:**A organização:  
  
a. Mantém os níveis de temperatura e umidade dentro da instalação onde o sistema de informações reside em [Atribuição: níveis aceitáveis definidos pela organização]; e  
  
b. Monitora os níveis de temperatura e umidade [Tarefa: frequência definida pela organização].  
  
**Guia Adicional:**Esse controle se aplica principalmente a instalações que contêm concentrações de recursos do sistema de informações, por exemplo, datacenters, salas de servidores e salas de computadores de mainframe.  
  
**Melhorias do Controle:**

### PE-14(1): Controles de Temperatura e Umidade | Controles Automáticos

A organização emprega controles automáticos de temperatura e umidade nas instalações para evitar flutuações potencialmente prejudiciais ao sistema de informação.

### PE-14(2): Controles de Temperatura e Umidade | Monitoramento com Alarmes / Notificações

A organização emprega monitoramento de temperatura e umidade que fornece um alarme ou notificação de alterações potencialmente prejudiciais ao pessoal ou equipamento.

## PE-15: Proteção de Danos a Água (P1)

**Descrição do Controle:**A organização protege o sistema de informações contra danos resultantes de vazamento de água, fornecendo válvulas mestra de fechamento ou isolamento acessíveis, funcionando corretamente e conhecidas pelo pessoal-chave.  
  
**Guia Adicional:**Esse controle se aplica principalmente a instalações que contêm concentrações de recursos do sistema de informações, incluindo, por exemplo, centros de dados, salas de servidores e salas de computadores de mainframe. Válvulas de isolamento podem ser empregadas além ou no lugar de válvulas de fechamento mestre para interromper o abastecimento de água em áreas específicas de interesse, sem afetar organizações inteiras.  
  
**Melhorias do Controle:**

### PE-15(1): Proteção de Danos a Água | Suporte à Automação

A organização emprega mecanismos automatizados para detectar a presença de água nas proximidades do sistema de informações e alerta [Atribuição: pessoal ou funções definidas pela organização].  
Guia Adicional: Mecanismos automatizados podem incluir, por exemplo, sensores de detecção de água, alarmes e sistemas de notificação.

## PE-16: Entrega e Remoção (P2)

**Descrição do Controle:**A organização autoriza, monitora e controla [Atribuição: tipos definidos pela organização de componentes do sistema de informações] entrando e saindo da instalação e mantém registros desses itens.  
  
**Guia Adicional:**A aplicação efetiva de autorizações para entrada e saída de componentes do sistema de informações pode exigir a restrição do acesso às áreas de entrega e, possivelmente, isolar as áreas do sistema de informações e das bibliotecas de mídia.

## PE-17: Local de Trabalho Alternativo (P2)

**Descrição do Controle:**A organização:  
  
a. Emprega [atribuição: controles de segurança definidos pela organização] em locais de trabalho alternativos;  
  
b. Considera possível, a eficácia dos controles de segurança em locais de trabalho alternativos; e  
  
c. Fornece um meio para os funcionários se comunicarem com o pessoal de segurança da informação em caso de incidentes ou problemas de segurança.  
  
**Guia Adicional:**Locais de trabalho alternativos podem incluir, por exemplo, instalações governamentais ou residências particulares de funcionários. Embora geralmente sejam distintos dos locais de processamento alternativos, os locais de trabalho alternativos podem fornecer locais alternativos prontamente disponíveis como parte das operações de contingência. As organizações podem definir diferentes conjuntos de controles de segurança para sites de trabalho alternativos específicos ou tipos de sites, dependendo das atividades relacionadas ao trabalho realizadas nesses sites. Esse controle suporta as atividades de planejamento de contingência das organizações e a iniciativa federal de telecomunicação.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-46 | https://csrc.nist.gov/publications/search?keywords-lg=800-46 |

## PE-18: Localização dos Componentes do Sistema de Informação (P3)

**Descrição do Controle:**A organização posiciona os componentes do sistema de informações dentro da instalação para minimizar possíveis danos causados por [Atribuição: riscos físicos e ambientais definidos pela organização] e para minimizar a oportunidade de acesso não autorizado.  
  
**Guia Adicional:**Os riscos físicos e ambientais incluem, por exemplo, inundações, incêndios, tornados, terremotos, furacões, atos de terrorismo, vandalismo, pulso eletromagnético, interferência elétrica e outras formas de radiação eletromagnética recebida. Além disso, as organizações consideram a localização dos pontos de entrada físicos onde indivíduos não autorizados, embora não tenham acesso concedido, podem estar muito próximos dos sistemas de informação e, portanto, aumentar o potencial de acesso não autorizado às comunicações organizacionais (por exemplo, através do uso de sniffers sem fio). ou microfones).  
  
**Melhorias do Controle:**

### PE-18(1): Localização dos Componentes do Sistema de Informação | Local da Instalação

A organização planeja a localização ou o local da instalação onde o sistema de informações reside em relação aos riscos físicos e ambientais e para as instalações existentes, considera os riscos físicos e ambientais em sua estratégia de mitigação de riscos.

## PE-19: Vazamento de Informação (P0)

**Descrição do Controle:**A organização protege o sistema de informações contra vazamento de informações devido a emanações de sinais eletromagnéticos.  
  
**Guia Adicional:**Vazamento de informações é a liberação intencional ou não intencional de informações para um ambiente não confiável a partir de emanações de sinais eletromagnéticos. Categorias de segurança ou classificações de sistemas de informação (com relação à confidencialidade) e políticas de segurança organizacionais orientam a seleção de controles de segurança empregados para proteger os sistemas contra vazamento de informações devido a emanações de sinais eletromagnéticos.  
  
**Melhorias do Controle:**

### PE-19(1): Vazamento de Informação | Emissões Nacionais / Políticas e Procedimentos de Tempestade

A organização garante que os componentes do sistema de informação, as comunicações de dados associadas e as redes sejam protegidos de acordo com as políticas e procedimentos nacionais de emissões e TEMPEST, com base na categoria ou classificação de segurança das informações.

**Referências:**

|  |  |
| --- | --- |
| Publicações de Normas Federais de Processamento de Informações N.199 | http://csrc.nist.gov/publications/PubsFIPS.html#199 |

## PE-20: Monitoramento e Acompanhamento de Ativos (P0)

**Descrição do Controle:**A organização:  
  
a. Emprega [Cessão: tecnologias de localização de ativos definidos pela organização] para rastrear e monitorar o local e o movimento de [Cessão: ativos definidos pela organização] dentro de [Cessão: áreas controladas definidas pela organização]; e  
  
b. Garante que as tecnologias de localização de ativos sejam empregadas de acordo com as leis federais aplicáveis, ordens executivas, diretrizes, regulamentos, políticas, normas e orientações.  
  
**Guia Adicional:**As tecnologias de localização de ativos podem ajudar as organizações a garantir que ativos críticos, como veículos ou componentes essenciais do sistema de informações, permaneçam em locais autorizados. As organizações consultam o Escritório do Conselho Geral e o Oficial Sênior da Agência para Privacidade (SAOP) / Diretor de Privacidade (CPO) sobre a implantação e o uso de tecnologias de localização de ativos para tratar de possíveis problemas de privacidade.

# PL - Planejamento

## PL-1: Política e Procedimentos do Planejamento de Segurança (P1)

**Descrição do Controle:**A organização:  
  
a. Desenvolve, documenta e divulga para [Atribuição: pessoal ou funções definidas pela organização]:  
  
1. Uma política de planejamento de segurança que atenda a finalidade, escopo, funções, responsabilidades, compromisso de gerenciamento, coordenação entre entidades organizacionais e conformidade; e  
  
2. Procedimentos para facilitar a implementação da política de planejamento de segurança e dos controles de planejamento de segurança associados; e  
  
b. Analisa e atualiza a atual:  
  
1. Política de planejamento de segurança [Atribuição: frequência definida pela organização]; e  
  
2. Procedimentos de planejamento de segurança [Atribuição: frequência definida pela organização].  
  
**Guia Adicional:**Esse controle trata do estabelecimento de políticas e procedimentos para a implementação efetiva de controles de segurança selecionados e aprimoramentos de controle na família PL. As políticas e procedimentos refletem as leis federais aplicáveis, ordens executivas, diretivas, regulamentos, políticas, normas e diretrizes. Políticas e procedimentos do programa de segurança no nível da organização podem tornar desnecessária a necessidade de políticas e procedimentos específicos do sistema. A política pode ser incluída como parte da política geral de segurança da informação para organizações ou, inversamente, pode ser representada por múltiplas políticas refletindo a natureza complexa de certas organizações. Os procedimentos podem ser estabelecidos para o programa de segurança em geral e para sistemas de informação específicos, se necessário. A estratégia de gerenciamento de risco organizacional é um fator chave no estabelecimento de políticas e procedimentos.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-12 | https://csrc.nist.gov/publications/search?keywords-lg=800-12 |
| Publicação Especial NIST 800-18 | https://csrc.nist.gov/publications/search?keywords-lg=800-18 |
| Publicação Especial NIST 800-100 | https://csrc.nist.gov/publications/search?keywords-lg=800-100 |

## PL-2: Plano de Segurança do Sistema (P1)

**Descrição do Controle:**A organização:  
  
a. Desenvolve um plano de segurança para o sistema de informações que:  
  
1. É consistente com a arquitetura corporativa da organização;  
  
2. Define explicitamente o limite de autorização para o sistema;  
  
3. Descreve o contexto operacional do sistema de informação em termos de missões e processos de negócios;  
  
4. Fornece a categorização de segurança do sistema de informações, incluindo a justificativa de suporte;  
  
5. Descreve o ambiente operacional do sistema de informação e os relacionamentos ou conexões com outros sistemas de informação;  
  
6. Fornece uma visão geral dos requisitos de segurança do sistema;  
  
7. Identifica quaisquer sobreposições relevantes, se aplicável;  
  
8. Descreve os controles de segurança em vigor ou planejados para atender a esses requisitos, incluindo uma justificativa para as decisões de adaptação; e  
  
9. É revisado e aprovado pelo oficial autorizador ou representante designado antes da implementação do plano;  
  
b. Distribui cópias do plano de segurança e comunica alterações subsequentes ao plano para [Atribuição: pessoal ou funções definidas pela organização];  
  
c. Revisa o plano de segurança do sistema de informações [Atribuição: frequência definida pela organização];  
  
d. Atualiza o plano para tratar de alterações no sistema de informações / ambiente de operação ou problemas identificados durante a implementação do plano ou avaliações de controle de segurança; e  
  
e. Protege o plano de segurança contra divulgação e modificação não autorizadas.  
  
**Guia Adicional:**Os planos de segurança relacionam os requisitos de segurança a um conjunto de controles e aprimoramentos de controle. Os planos de segurança também descrevem, em alto nível, como os controles e aprimoramentos de controle atendem a esses requisitos de segurança, mas não fornecem descrições técnicas detalhadas do design ou implementação específica dos controles / aprimoramentos. Os planos de segurança contêm informações suficientes (incluindo a especificação de valores de parâmetros para instruções de atribuição e seleção, de forma explícita ou por referência) para permitir um design e implementação que sejam inequivocamente compatíveis com a intenção dos planos e determinações subsequentes de risco para operações e ativos organizacionais, indivíduos, outras organizações e a Nação, se o plano for implementado conforme o planejado. As organizações também podem aplicar orientações de adaptação às linhas de base de controle de segurança no Apêndice D e na Instrução CNSS 1253 para desenvolver sobreposições para uso em toda a comunidade ou abordar requisitos, tecnologias ou missões / ambientes de operação especializados (por exemplo, DoD-tático, Chave Pública Federal Infraestrutura, ou Federal Identity, Credential, and Access Management, operações espaciais). O Apêndice I fornece orientação sobre o desenvolvimento de sobreposições. Os planos de segurança não precisam ser documentos únicos; os planos podem ser uma coleção de vários documentos, incluindo documentos que já existem. Planos de segurança eficazes fazem uso extensivo de referências a políticas, procedimentos e documentos adicionais (por exemplo, especificações de design e implementação), onde informações mais detalhadas podem ser obtidas. Isso reduz os requisitos de documentação associados aos programas de segurança e mantém as informações relacionadas à segurança em outras áreas operacionais / de gerenciamento estabelecidas relacionadas à arquitetura corporativa, ciclo de vida de desenvolvimento do sistema, engenharia de sistemas e aquisição. Por exemplo, os planos de segurança não contêm informações detalhadas do plano de contingência ou do plano de resposta a incidentes, mas fornecem explicitamente ou por referência informações suficientes para definir o que precisa ser realizado por esses planos.  
  
**Melhorias do Controle:**

### PL-2(1): Plano de Segurança do Sistema | Conceito de Operações

[Retirado: Incorporado ao PL-7].

### PL-2(2): Plano de Segurança do Sistema | Arquitetura Funcional

[Retirado: Incorporado ao PL-8].

### PL-2(3): Plano de Segurança do Sistema | Planejar / Coordenar com Outras Entidades Organizacionais

A organização planeja e coordena as atividades relacionadas à segurança que afetam o sistema de informação com [Atribuição: indivíduos ou grupos definidos pela organização] antes de realizar essas atividades, a fim de reduzir o impacto em outras entidades organizacionais.  
Guia Adicional: As atividades relacionadas à segurança incluem, por exemplo, avaliações de segurança, auditorias, manutenção de hardware e software, gerenciamento de patches e teste de plano de contingência. O planejamento e a coordenação avançados incluem situações de emergência e não-emergência (isto é, não planejadas ou não emergentes). O processo definido pelas organizações para planejar e coordenar atividades relacionadas à segurança pode ser incluído nos planos de segurança para sistemas de informação ou outros documentos, conforme apropriado.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-18 | https://csrc.nist.gov/publications/search?keywords-lg=800-18 |

## PL-3: Atualização do Plano de Segurança do Sistema (P0)

**Descrição do Controle:**[Retirado: Incorporado ao PL-2].

## PL-4: Regras de Comportamento (P2)

**Descrição do Controle:**A organização:  
  
a. Estabelece e torna prontamente disponível para indivíduos que necessitam de acesso ao sistema de informação, as regras que descrevem suas responsabilidades e o comportamento esperado em relação ao uso de informações e sistemas de informação;  
  
b. Recebe um reconhecimento assinado de tais indivíduos, indicando que eles leram, entendem e concordam em cumprir as regras de comportamento antes de autorizar o acesso às informações e ao sistema de informações;  
  
c. Revisa e atualiza as regras de comportamento [Atribuição: frequência definida pela organização]; e  
  
d. Requer que os indivíduos que assinaram uma versão anterior das regras de comportamento leiam e assinem novamente quando as regras de comportamento forem revisadas / atualizadas.  
  
**Guia Adicional:**Esse aprimoramento de controle se aplica aos usuários organizacionais. As organizações consideram regras de comportamento com base nas funções e responsabilidades individuais dos usuários, diferenciando, por exemplo, entre regras que se aplicam a usuários privilegiados e regras que se aplicam a usuários gerais. Estabelecer regras de comportamento para alguns tipos de usuários não organizacionais, incluindo, por exemplo, indivíduos que simplesmente recebem dados / informações de sistemas de informações federais, muitas vezes não é viável, dado o grande número desses usuários e a natureza limitada de suas interações com os sistemas. Regras de comportamento para usuários organizacionais e não organizacionais também podem ser estabelecidas no AC-8, Notificação de uso do sistema. PL-4 b. (a parte de reconhecimento assinado deste controle) pode ser satisfeita pelo treinamento de conscientização de segurança e pelos programas de treinamento em segurança baseados em funções, conduzidos pelas organizações, se esse treinamento incluir regras de comportamento. As organizações podem usar assinaturas eletrônicas para reconhecer regras de comportamento.  
  
**Melhorias do Controle:**

### PL-4(1): Regras de Comportamento | Mídia Social e Restrições de Rede

A organização inclui nas regras de comportamento, restrições explícitas ao uso de mídias sociais / sites de redes e publicação de informações organizacionais em sites públicos.  
Guia Adicional: Esse aprimoramento de controle trata das regras de comportamento relacionadas ao uso de sites de redes sociais / redes: (i) quando o pessoal da organização está usando esses sites para tarefas oficiais ou na condução de negócios oficiais; (ii) quando informações organizacionais estiverem envolvidas em transações de redes sociais / redes; e (iii) quando o pessoal estiver acessando sites de redes sociais / redes a partir de sistemas de informações organizacionais. As organizações também abordam regras específicas que impedem que entidades não autorizadas obtenham e/ou deduzam informações organizacionais não públicas (por exemplo, informações de contas do sistema, informações de identificação pessoal) de sites de redes sociais / redes.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-18 | https://csrc.nist.gov/publications/search?keywords-lg=800-18 |

## PL-5: Avaliação de Impacto de Privacidade (P0)

**Descrição do Controle:**[Retirado: Incorporado no Apêndice J, AR-2].

## PL-6: Planejamento de Atividades Relacionadas com a Segurança (P0)

**Descrição do Controle:**[Retirado: Incorporado ao PL-2].

## PL-7: Conceito de Segurança das Operações (P0)

**Descrição do Controle:**A organização:  
  
a. Desenvolve um Conceito de Operações de Segurança (CONOPS) para o sistema de informações que contém, no mínimo, como a organização pretende operar o sistema da perspectiva da segurança da informação; e  
  
b. Revisa e atualiza os CONOPS [Atribuição: frequência definida pela organização].  
  
**Guia Adicional:**Os CONOPS de segurança podem ser incluídos no plano de segurança do sistema de informações ou em outros documentos relacionados ao ciclo de vida de desenvolvimento do sistema, conforme apropriado. As alterações no CONOPS são refletidas nas atualizações contínuas do plano de segurança, da arquitetura de segurança da informação e de outros documentos organizacionais apropriados (por exemplo, especificações de segurança para compras / aquisições, documentos do ciclo de vida de desenvolvimento do sistema e documentos de engenharia de sistemas / segurança).

## PL-8: Arquitetura de Segurança da Informação (P1)

**Descrição do Controle:**A organização:  
  
a. Desenvolve uma arquitetura de segurança da informação para o sistema de informação que:  
  
1. Descreve a filosofia, os requisitos e a abordagem gerais a serem adotados em relação à proteção da confidencialidade, integridade e disponibilidade das informações organizacionais;  
  
2. Descreve como a arquitetura de segurança da informação é integrada e suporta a arquitetura corporativa; e  
  
3. Descreve quaisquer premissas de segurança da informação sobre e dependências de serviços externos;  
  
b. Revisa e atualiza a arquitetura de segurança da informação [Atribuição: frequência definida pela organização] para refletir as atualizações na arquitetura corporativa; e  
  
c. Garante que as mudanças planejadas na arquitetura de segurança das informações sejam refletidas no plano de segurança, no CONOPS (conceito de operações de segurança) e nas aquisições / aquisições organizacionais.  
  
**Guia Adicional:**Esse controle aborda as ações executadas pelas organizações no design e desenvolvimento de sistemas de informação. A arquitetura de segurança da informação no nível do sistema de informação individual é consistente e complementa a arquitetura de segurança da informação mais global, descrita na PM-7, que é parte integrante e desenvolvida como parte da arquitetura corporativa. A arquitetura de segurança da informação inclui uma descrição da arquitetura, o posicionamento / alocação da funcionalidade de segurança (incluindo controles de segurança), informações relacionadas à segurança para interfaces externas, informações sendo trocadas entre as interfaces e os mecanismos de proteção associados a cada interface. Além disso, a arquitetura de segurança pode incluir outras informações importantes relacionadas à segurança, por exemplo, funções de usuário e privilégios de acesso atribuídos a cada função, requisitos de segurança exclusivos, tipos de informações processadas, armazenadas e transmitidas pelo sistema de informação, prioridades de restauração de serviços de informações e sistemas de informações e quaisquer outras necessidades específicas de proteção. Na arquitetura moderna de hoje, está se tornando menos comum para as organizações controlar todos os recursos de informação. Haverá dependências importantes em serviços de informações externas e provedores de serviços. A descrição de tais dependências na arquitetura de segurança da informação é importante para o desenvolvimento de uma estratégia abrangente de proteção de missão / negócios. Estabelecendo, desenvolvendo, documentando e mantendo sob controle de configuração, uma configuração de linha de base para sistemas de informações organizacionais é essencial para implementar e manter uma arquitetura de segurança da informação eficaz. O desenvolvimento da arquitetura de segurança da informação é coordenado com o Oficial Sênior da Agência para Privacidade (SAOP) / Chief Privacy Officer (CPO) para garantir que os controles de segurança necessários para dar suporte aos requisitos de privacidade sejam identificados e implementados com eficácia. O PL-8 é direcionado principalmente às organizações (ou seja, com foco interno) para ajudar a garantir que as organizações desenvolvam uma arquitetura de segurança da informação para o sistema de informações e que a arquitetura de segurança seja integrada ou fortemente acoplada à arquitetura corporativa por meio das informações da arquitetura de segurança de toda a organização. Por outro lado, o SA-17 é direcionado principalmente a desenvolvedores e integradores externos de produtos / sistemas de tecnologia da informação (embora o SA-17 possa ser usado internamente nas organizações para o desenvolvimento interno de sistemas). O SA-17, que é complementar ao PL-8, é selecionado quando as organizações terceirizam o desenvolvimento de sistemas de informações ou componentes de sistemas de informações para entidades externas, e é necessário demonstrar / mostrar consistência com a arquitetura corporativa da organização e a arquitetura de segurança da informação.  
  
**Melhorias do Controle:**

### PL-8(1): Arquitetura de Segurança da Informação | Defesa em Profundidade

A organização projeta sua arquitetura de segurança usando uma abordagem de defesa profunda que:  
  
a. Aloca [Atribuição: salvaguardas de segurança definidas pela organização] para [Atribuição: locais definidos pela organização e camadas arquiteturais]; e  
  
b. Garante que as salvaguardas de segurança alocadas operem de maneira coordenada e que se reforce mutuamente.  
Guia Adicional: As organizações alocam estrategicamente salvaguardas de segurança (procedurais, técnicas ou ambas) na arquitetura de segurança, para que os adversários tenham que superar várias salvaguardas para atingir seu objetivo. Exigir que os adversários derrotem vários mecanismos torna mais difícil o ataque bem-sucedido de recursos críticos de informação (ou seja, aumenta o fator de trabalho adverso) e também aumenta a probabilidade de detecção. A coordenação das salvaguardas alocadas é essencial para garantir que um ataque que envolva uma salvaguarda não crie consequências indesejadas adversas (por exemplo, bloqueio, alarmes em cascata), interferindo em outra salvaguarda. A colocação de salvaguardas de segurança é uma atividade essencial. Maior criticidade de ativos ou valor das informações merece camadas adicionais. Assim, uma organização pode optar por colocar o software antivírus nas camadas limites organizacionais, servidores de e-mail / web, notebooks e estações de trabalho para maximizar o número de salvaguardas relacionadas que os adversários devem penetrar antes de comprometer as informações e os sistemas de informação.

### PL-8(2): Arquitetura de Segurança da Informação | Diversidade de Fornecedores

A organização exige que [Atribuição: salvaguardas de segurança definidas pela organização] alocadas a [Atribuição: locais definidos pela organização e camadas arquitetônicas] sejam obtidas de diferentes fornecedores.  
Guia Adicional: Diferentes produtos de tecnologia da informação têm diferentes pontos fortes e fracos. O fornecimento de um amplo espectro de produtos complementa as ofertas individuais. Por exemplo, os fornecedores que oferecem proteção de código mal-intencionado geralmente atualizam seus produtos em momentos diferentes, geralmente desenvolvendo soluções para vírus, cavalos de Troia ou worms conhecidos, de acordo com suas prioridades e cronogramas de desenvolvimento. Por ter produtos diferentes em locais diferentes (por exemplo, servidor, limite, área de trabalho), há uma probabilidade maior de que pelo menos um deles detecte o código malicioso.

## PL-9: Gestão Central (P0)

**Descrição do Controle:**A organização gerencia centralmente [Atribuição: controles de segurança definidos pela organização e processos relacionados].  
  
**Guia Adicional:**Gerenciamento central refere-se ao gerenciamento e implementação em toda a organização de controles de segurança selecionados e processos relacionados. O gerenciamento central inclui planejar, implementar, avaliar, autorizar e monitorar os controles e processos de segurança gerenciados e definidos pela organização. Como o gerenciamento central de controles de segurança geralmente é associado a controles comuns, esse gerenciamento promove e facilita a padronização das implementações de controle de segurança e o gerenciamento e o uso criterioso dos recursos organizacionais. Os controles e processos de segurança gerenciados centralmente também podem atender aos requisitos de independência para avaliações de suporte às autorizações iniciais e contínuas para operar como parte do monitoramento contínuo organizacional. Como parte do processo de seleção do controle de segurança, as organizações determinam quais controles podem ser adequados para o gerenciamento central com base nos recursos e capacidades organizacionais. As organizações consideram que nem sempre é possível gerenciar centralmente todos os aspectos de um controle de segurança. Nesses casos, o controle de segurança é tratado como um controle híbrido, com o controle gerenciado e implementado centralmente ou no nível do sistema de informações. Os controles e aprimoramentos de controle candidatos ao gerenciamento central total ou parcial incluem, mas não estão limitados a: AC-2 (1) (2) (3) (4); AC-17 (1) (2) (3) (9); AC-18 (1) (3) (4) (5); AC-19 (4); AC-22; AC-23; AT-2 (1) (2); AT-3 (1) (2) (3); AT-4; AU-6 (1) (3) (5) (6) (9); AU-7 (1) (2); AU-11, AU-13, AU-16, CA-2 (1) (2) (3); CA-3 (1) (2) (3); CA-7 (1); CA-9; CM-2 (1) (2); CM-3 (1) (4); CM-4; CM-6 (1); CM-7 (4) (5); CM-8 (todos); CM-9 (1); CM-10; CM-11; CP-7 (todos); CP-8 (todos); SC-43; SI-2; SI-3; SI-7; e SI-8.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-37 | https://csrc.nist.gov/publications/search?keywords-lg=800-37 |

# PM - Gestão de Programas

## PM-1: Plano do Programa de Segurança da Informação (P0)

**Descrição do Controle:**A organização:  
  
a. Desenvolve e divulga um plano de programa de segurança da informação em toda a organização que:  
  
1. Fornece uma visão geral dos requisitos do programa de segurança e uma descrição dos controles de gerenciamento do programa de segurança e controles comuns em vigor ou planejados para atender a esses requisitos;  
  
2. Inclui a identificação e atribuição de funções, responsabilidades, compromisso de gestão, coordenação entre entidades organizacionais e conformidade;  
  
3. Reflete a coordenação entre as entidades organizacionais responsáveis pelos diferentes aspectos da segurança da informação (isto é, técnico, físico, pessoal, cyber-físico); e  
  
4. É aprovado por um funcionário sênior com responsabilidade e prestação de contas pelo risco incorrido em operações organizacionais (incluindo missão, funções, imagem e reputação), ativos organizacionais, indivíduos, outras organizações e a Nação;  
  
b. Revisa o plano do programa de segurança da informação em toda a organização [Atribuição: frequência definida pela organização];  
  
c. Atualiza o plano para tratar de alterações e problemas organizacionais identificados durante a implementação do plano ou avaliações de controle de segurança; e  
  
d. Protege o plano do programa de segurança da informação contra divulgação e modificação não autorizadas.  
  
**Guia Adicional:**Os planos do programa de segurança da informação podem ser representados em documentos únicos ou compilações de documentos, a critério das organizações. Os planos documentam os controles de gerenciamento do programa e os controles comuns definidos pela organização. Os planos do programa de segurança da informação fornecem informações suficientes sobre os controles de gerenciamento do programa / controles comuns (incluindo a especificação de parâmetros para quaisquer instruções de designação e seleção, explicitamente ou por referência) para permitir implementações que sejam inequivocamente compatíveis com a intenção dos planos e uma determinação do risco a incorrer se os planos forem implementados conforme o planejado. Os planos de segurança para sistemas de informações individuais e o programa de segurança da informação em toda a organização, juntos, oferecem cobertura completa para todos os controles de segurança empregados na organização. Os controles comuns estão documentados em um apêndice do plano de programa de segurança da informação da organização, a menos que os controles sejam incluídos em um plano de segurança separado para um sistema de informações (por exemplo, controles de segurança empregados como parte de um sistema de detecção de intrusão que fornece proteção de limites em toda a organização herdada por um ou mais sistemas de informação organizacional). O plano do programa de segurança da informação em toda a organização indicará quais planos de segurança separados contêm descrições de controles comuns. As organizações têm a flexibilidade de descrever controles comuns em um único documento ou em vários documentos. No caso de vários documentos, os documentos que descrevem controles comuns são incluídos como anexos ao plano do programa de segurança da informação. Se o plano do programa de segurança da informação contiver vários documentos, a organização especificará em cada documento o funcionário ou funcionários da organização responsáveis pelo desenvolvimento, implementação, avaliação, autorização e monitoramento dos respectivos controles comuns. Por exemplo, a organização pode exigir que o Escritório de Gerenciamento de Instalações desenvolva, implemente, avalie, autorize e monitore continuamente controles comuns de proteção física e ambiental da família PE quando esses controles não estiverem associados a um sistema de informações específico, mas, ao invés disso, suportem várias informações sistemas.

## PM-2: Diretor de Segurança de Informação Sênior (P0)

**Descrição do Controle:**A organização nomeia um oficial sênior de segurança da informação com a missão e os recursos para coordenar, desenvolver, implementar e manter um programa de segurança da informação em toda a organização.  
  
**Guia Adicional:**O oficial de segurança descrito neste controle é um oficial da organização. Para uma agência federal (conforme definido nas leis federais aplicáveis, ordens executivas, diretrizes, políticas ou regulamentos), esse funcionário é o oficial sênior de segurança da informação da agência. As organizações também podem se referir a esse funcionário como Diretor Sênior de Segurança da Informação ou Diretor de Segurança da Informação.

## PM-3: Recursos de Segurança da Informação (P0)

**Descrição do Controle:**A organização:  
  
a. Garante que todas as solicitações de planejamento e investimento de capital incluam os recursos necessários para implementar o programa de segurança da informação e documentem todas as exceções a esse requisito;  
  
b. Emprega um caso de negócios / Anexo 300 / Anexo 53 para registrar os recursos necessários; e  
  
c. Garante que os recursos de segurança da informação estejam disponíveis para as despesas, conforme planejado.  
  
**Guia Adicional:**As organizações consideram o estabelecimento de defensores dos esforços de segurança da informação e, como parte da inclusão dos recursos necessários, atribuem conhecimentos especializados e recursos, conforme necessário. As organizações podem designar e capacitar um Conselho de Revisão de Investimentos (ou grupo similar) para gerenciar e supervisionar os aspectos relacionados à segurança da informação do processo de planejamento de capital e controle de investimentos.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-65 | https://csrc.nist.gov/publications/search?keywords-lg=800-65 |

## PM-4: Plano de Ação e Marcos do Processo (P0)

**Descrição do Controle:**A organização:  
  
a. Implementa um processo para garantir que os planos de ação e os marcos para o programa de segurança e os sistemas de informações organizacionais associados:  
  
1. sejam desenvolvidos e mantidos;  
  
2. Documentar as ações corretivas de segurança da informação para responder adequadamente aos riscos de operações e ativos organizacionais, indivíduos, outras organizações e a Nação; e  
  
3. São relatados de acordo com os requisitos de relatório do OMB FISMA.  
  
b. Revisa os planos de ação e os marcos para obter consistência com a estratégia de gerenciamento de riscos organizacionais e as prioridades da organização para ações de resposta a riscos.  
  
**Guia Adicional:**O plano de ação e os marcos são um documento essencial no programa de segurança da informação e estão sujeitos aos requisitos de relatórios federais estabelecidos pela OMB. Com a ênfase crescente no gerenciamento de riscos em toda a organização em todas as três camadas da hierarquia de gerenciamento de riscos (organização, missão / processos de negócios e sistema de informação), as organizações visualizam planos de ação e marcos da perspectiva organizacional, priorizando ações de resposta a riscos e garantir consistência com as metas e objetivos da organização. As atualizações do plano de ação e dos marcos são baseadas nas descobertas das avaliações de controle de segurança e nas atividades de monitoramento contínuo. As diretrizes de relatórios do OMB FISMA contêm instruções sobre os planos de ação organizacionais e os marcos.

**Referências:**

|  |  |
| --- | --- |
| OMB Memorando 02-01 | https://georgewbush-whitehouse.archives.gov/omb/memoranda/m02-01.html |
| Publicação Especial NIST 800-37 | https://csrc.nist.gov/publications/search?keywords-lg=800-37 |

## PM-5: Inventário do Sistema de Informação (P0)

**Descrição do Controle:**A organização desenvolve e mantém um inventário de seus sistemas de informação.  
  
**Guia Adicional:**Este controle aborda os requisitos de inventário no FISMA. O OMB fornece orientação sobre o desenvolvimento de inventários de sistemas de informação e requisitos de relatórios associados. Para requisitos específicos de relatórios de inventário de sistemas de informações, as organizações consultam as orientações anuais de relatórios OMB FISMA.

**Referências:**

|  |  |
| --- | --- |
| OMB: Escritório de Gestão e Orçamento | https://www.whitehouse.gov/omb/ |

## PM-6: Medidas de Desempenho da Segurança da Informação (P0)

**Descrição do Controle:**A organização desenvolve, monitora e relata os resultados das medidas de desempenho de segurança da informação.  
  
**Guia Adicional:**Medidas de desempenho são métricas baseadas em resultados usadas por uma organização para medir a eficácia ou eficiência do programa de segurança da informação e dos controles de segurança empregados no suporte ao programa.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-55 | https://csrc.nist.gov/publications/search?keywords-lg=800-55 |

## PM-7: Arquitetura Empresarial (P0)

**Descrição do Controle:**A organização desenvolve uma arquitetura corporativa considerando a segurança da informação e o risco resultante para operações organizacionais, ativos organizacionais, indivíduos, outras organizações e a Nação.  
  
**Guia Adicional:**A arquitetura corporativa desenvolvida pela organização está alinhada com a Arquitetura Corporativa Federal. A integração de requisitos de segurança da informação e controles de segurança associados na arquitetura corporativa da organização ajuda a garantir que as considerações de segurança sejam abordadas pelas organizações no início do ciclo de vida do desenvolvimento do sistema e estejam direta e explicitamente relacionadas aos processos de missão / negócios da organização. Esse processo de integração de requisitos de segurança também se incorpora à arquitetura corporativa, uma arquitetura de segurança da informação integral consistente com o gerenciamento de riscos organizacionais e estratégias de segurança da informação. Para o PM-7, a arquitetura de segurança da informação é desenvolvida no nível do sistema de sistemas (em toda a organização), representando todos os sistemas de informações organizacionais. Para o PL-8, a arquitetura de segurança da informação é desenvolvida em um nível que representa um sistema de informações individual, mas, ao mesmo tempo, é consistente com a arquitetura de segurança da informação definida para a organização. Os requisitos de segurança e a integração do controle de segurança são cumpridos com mais eficiência através da aplicação da Estrutura de Gerenciamento de Riscos e do suporte a padrões e diretrizes de segurança. A Metodologia Federal de Arquitetura de Segmento fornece orientação sobre a integração de requisitos de segurança da informação e controles de segurança nas arquiteturas corporativas.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-39 | https://csrc.nist.gov/publications/search?keywords-lg=800-39 |

## PM-8: Plano de Infraestrutura Crítica (P0)

**Descrição do Controle:**A organização aborda questões de segurança da informação no desenvolvimento, documentação e atualização de uma infraestrutura crítica e de um plano de proteção de recursos importantes.  
  
**Guia Adicional:**As estratégias de proteção são baseadas na priorização de ativos e recursos críticos. O requisito e a orientação para definir a infraestrutura crítica e os principais recursos e para preparar um plano de proteção de infraestrutura crítica associado são encontrados nas leis federais aplicáveis, ordens executivas, diretrizes, políticas, regulamentos, normas e orientações.

**Referências:**

|  |  |
| --- | --- |
| DHS - HSPD-7 | https://www.dhs.gov/homeland-security-presidential-directive-7 |
| DHS - Plano Nacional de Proteção de Infraestrutura | https://www.dhs.gov/national-infrastructure-protection-plan |

## PM-9: Estratégia de Gestão de Riscos (P0)

**Descrição do Controle:**A organização:  
  
a. Desenvolve uma estratégia abrangente para gerenciar riscos para operações e ativos organizacionais, indivíduos, outras organizações e a Nação associada à operação e uso de sistemas de informação;  
  
b. Implementa a estratégia de gerenciamento de riscos de forma consistente em toda a organização; e  
  
c. Revisa e atualiza a estratégia de gerenciamento de riscos [Atribuição: frequência definida pela organização] ou conforme necessário, para tratar de mudanças organizacionais.  
  
**Guia Adicional:**Uma estratégia de gerenciamento de riscos em toda a organização inclui, por exemplo, uma expressão inequívoca da tolerância a riscos para a organização, metodologias aceitáveis de avaliação de riscos, estratégias de mitigação de riscos, um processo para avaliar consistentemente os riscos em toda a organização com relação à tolerância a riscos da organização e abordagens para monitorar riscos ao longo do tempo. O uso de uma função executiva de risco pode facilitar a aplicação consistente e em toda a organização da estratégia de gerenciamento de riscos. A estratégia de gerenciamento de riscos em toda a organização pode ser informada por informações relacionadas a riscos de outras fontes, internas e externas à organização, para garantir que a estratégia seja ampla e abrangente.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-30 | https://csrc.nist.gov/publications/search?keywords-lg=800-30 |
| Publicação Especial NIST 800-39 | https://csrc.nist.gov/publications/search?keywords-lg=800-39 |

## PM-10: Processo de Autorização de Segurança (P0)

**Descrição do Controle:**A organização:  
  
a. Gerencia (ou seja, documentos, trilhas e relatórios) o estado de segurança dos sistemas de informações organizacionais e os ambientes nos quais esses sistemas operam através de processos de autorização de segurança;  
  
b. Designa indivíduos para desempenhar funções e responsabilidades específicas no processo de gerenciamento de riscos organizacionais; e  
  
c. Integra totalmente os processos de autorização de segurança em um programa de gerenciamento de riscos em toda a organização.  
  
**Guia Adicional:**Os processos de autorização de segurança para sistemas de informação e ambientes de operação requerem a implementação de um processo de gerenciamento de riscos em toda a organização, uma Estrutura de Gerenciamento de Riscos e padrões e diretrizes de segurança associados. As funções específicas do processo de gerenciamento de riscos incluem um executivo (função) de risco organizacional e autoridades autorizadas designadas para cada sistema de informações organizacionais e provedor de controle comum. Os processos de autorização de segurança são integrados aos processos organizacionais de monitoramento contínuo para facilitar a compreensão e aceitação contínuas dos riscos para operações e ativos organizacionais, indivíduos, outras organizações e a Nação.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-37 | https://csrc.nist.gov/publications/search?keywords-lg=800-37 |
| Publicação Especial NIST 800-39 | https://csrc.nist.gov/publications/search?keywords-lg=800-39 |

## PM-11: Definição do Processo da Missão/Negócio (P0)

**Descrição do Controle:**A organização:  
  
a. Define os processos de missão / negócios, considerando a segurança da informação e o risco resultante para operações organizacionais, ativos organizacionais, indivíduos, outras organizações e a Nação; e  
  
b. Determina as necessidades de proteção de informações decorrentes dos processos de missão / negócios definidos e revisa os processos conforme necessário, até que as necessidades de proteção alcançáveis sejam obtidas.  
  
**Guia Adicional:**As necessidades de proteção da informação são capacidades necessárias, independentes da tecnologia, para combater ameaças a organizações, indivíduos ou a Nação por meio do comprometimento de informações (ou seja, perda de confidencialidade, integridade ou disponibilidade). As necessidades de proteção de informações derivam das necessidades de missão / negócios definidos pela organização, dos processos de missão / negócios selecionados para atender às necessidades declaradas e da estratégia de gerenciamento de riscos organizacionais. As necessidades de proteção de informações determinam os controles de segurança necessários para a organização e os sistemas de informações associados que dão suporte aos processos de missão / negócios. Inerente à definição das necessidades de proteção de informações de uma organização, está o entendimento do nível de impacto adverso que pode resultar se ocorrer um comprometimento das informações. O processo de categorização de segurança é usado para fazer essas determinações de impacto em potencial. As definições de missão / processos de negócios e os requisitos de proteção de informações associados são documentados pela organização de acordo com a política e procedimento da organização.

**Referências:**

|  |  |
| --- | --- |
| Publicações de Normas Federais de Processamento de Informações N.199 | http://csrc.nist.gov/publications/PubsFIPS.html#199 |
| Publicação Especial NIST 800-60 | https://csrc.nist.gov/publications/search?keywords-lg=800-60 |

## PM-12: Programa de Ameaças Internas (Insiders) (P0)

**Descrição do Controle:**A organização implementa um programa de ameaças internas que inclui uma equipe interdisciplinar de tratamento de incidentes de ameaças internas.  
  
**Guia Adicional:**As organizações que lidam com informações classificadas são obrigadas, de acordo com a Ordem Executiva 13587 e a Política Nacional de Ameaças Internas, a estabelecer programas de ameaças internas. Os padrões e diretrizes que se aplicam aos programas de ameaças internas em ambientes classificados também podem ser empregados de maneira eficaz para melhorar a segurança das Informações Não Classificadas Controladas em sistemas de segurança não nacionais. Os programas de ameaças internas incluem controles de segurança para detectar e impedir atividades internas maliciosas por meio da integração e análise centralizadas de informações técnicas e não técnicas para identificar possíveis problemas de ameaças internas. Um funcionário sênior da organização é designado pelo chefe do departamento / agência como o indivíduo responsável por implementar e supervisionar o programa. Além da capacidade centralizada de integração e análise, os programas de ameaças internas, no mínimo, preparam políticas e planos de implementação de ameaças de departamentos / agências, conduzem o monitoramento com base no host das atividades individuais de funcionários em computadores classificados de propriedade do governo, fornecem treinamento de conscientização sobre ameaças internas para funcionários, receba acesso às informações de todos os escritórios do departamento / agência (por exemplo, recursos humanos, segurança jurídica, física, segurança de pessoal, tecnologia da informação, segurança de sistemas de informação e aplicação da lei) para análise de ameaças internas e realize auto avaliações postura de ameaça privilegiada do departamento / agência. Os programas de ameaças internas podem aproveitar a existência de equipes que lidam com incidentes que as organizações já podem ter, como equipes de resposta a incidentes de segurança de computadores. Os registros de recursos humanos são especialmente importantes nesse esforço, pois há evidências convincentes para mostrar que alguns tipos de crimes internos geralmente são precedidos por comportamentos não técnicos no local de trabalho (por exemplo, padrões contínuos de comportamento descontente e conflitos com colegas de trabalho e outros colegas). Esses precursores podem informar e orientar melhor os funcionários da organização em esforços de monitoramento mais focados e direcionados. A participação de uma equipe jurídica é importante para garantir que todas as atividades de monitoramento sejam realizadas de acordo com a legislação, diretrizes, regulamentos, políticas, normas e diretrizes apropriadas.

**Referências:**

|  |  |
| --- | --- |
| Ordem Executiva da Casa Branca Nº13587 | http://www.whitehouse.gov/the-press-office/2011/10/07/executive-order-13587-structural-reforms-improve-security-classified-net |

## PM-13: Força de Trabalho de Segurança da Informação (P0)

**Descrição do Controle:**A organização estabelece um programa de desenvolvimento e aprimoramento da força de trabalho de segurança da informação  
  
**Guia Adicional:**Os programas de desenvolvimento e aprimoramento da força de trabalho de segurança da informação incluem, por exemplo: (i) definição dos níveis de conhecimento e habilidade necessários para executar tarefas e tarefas de segurança da informação; (ii) desenvolvimento de programas de treinamento baseados em funções para indivíduos atribuídos a funções e responsabilidades de segurança da informação; e (iii) fornecer padrões para medir e criar qualificações individuais para titulares e candidatos a cargos relacionados à segurança da informação. Esses programas de força de trabalho também podem incluir planos de carreira de segurança da informação associados para incentivar: (i) profissionais de segurança da informação a avançar no campo e preencher cargos com maior responsabilidade; e (ii) organizações para preencher cargos relacionados à segurança da informação com pessoal qualificado. Os programas de desenvolvimento e aprimoramento da força de trabalho de segurança da informação são complementares aos programas de conscientização e treinamento em segurança organizacional. Os programas de desenvolvimento e aprimoramento da força de trabalho de segurança da informação concentram-se no desenvolvimento e na institucionalização dos principais recursos de segurança da informação do pessoal selecionado, necessário para proteger operações, ativos e indivíduos organizacionais.

## PM-14: Teste, Treinamento e Monitoramento (P0)

**Descrição do Controle:**A organização:  
  
a. Implementa um processo para garantir que os planos organizacionais para a realização de atividades de teste, treinamento e monitoramento de segurança associados aos sistemas de informações organizacionais:  
  
1. São desenvolvidos e mantidos; e  
  
2. Continuar a ser executado em tempo hábil;  
  
b. Revisa os planos de teste, treinamento e monitoramento para obter consistência com a estratégia de gerenciamento de riscos organizacionais e as prioridades da organização para ações de resposta a riscos.  
  
**Guia Adicional:**Esse controle garante que as organizações supervisionem as atividades de teste, treinamento e monitoramento de segurança realizadas em toda a organização e que essas atividades sejam coordenadas. Com a importância de programas de monitoramento contínuo, a implementação da segurança da informação nas três camadas da hierarquia de gerenciamento de riscos e o uso generalizado de controles comuns, as organizações coordenam e consolidam as atividades de teste e monitoramento que são rotineiramente conduzidas como parte das avaliações organizacionais em andamento, suportando uma variedade de controles de segurança. As atividades de treinamento em segurança, embora tipicamente focadas em sistemas de informações individuais e funções específicas, também exigem coordenação em todos os elementos organizacionais. Planos e atividades de teste, treinamento e monitoramento são informados pelas avaliações atuais de ameaças e vulnerabilidades.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-16 | https://csrc.nist.gov/publications/search?keywords-lg=800-16 |
| Publicação Especial NIST 800-39 | https://csrc.nist.gov/publications/search?keywords-lg=800-39 |
| Publicação Especial NIST 800-53A | https://csrc.nist.gov/publications/search?keywords-lg=800-53A |
| Publicação Especial NIST 800-137 | https://csrc.nist.gov/publications/search?keywords-lg=800-137 |

## PM-15: Contatos com Grupos de Segurança e Associações (P0)

**Descrição do Controle:**A organização estabelece e institucionaliza o contato com grupos e associações selecionados da comunidade de segurança:  
  
a. Facilitar a educação e o treinamento contínuos em segurança para o pessoal organizacional;  
  
b. Manter a moeda com práticas, técnicas e tecnologias de segurança recomendadas; e  
  
c. Compartilhar informações atuais relacionadas à segurança, incluindo ameaças, vulnerabilidades e incidentes.  
  
**Guia Adicional:**O contato contínuo com grupos e associações de segurança é de suma importância em um ambiente de ameaças e tecnologias em rápida mudança. Grupos e associações de segurança incluem, por exemplo, grupos de interesse especial, fóruns, associações profissionais, grupos de notícias e/ou grupos de profissionais de segurança em organizações semelhantes. As organizações selecionam grupos e associações com base em missões organizacionais / funções de negócios. As organizações compartilham informações sobre ameaças, vulnerabilidades e incidentes, de acordo com as leis federais aplicáveis, ordens executivas, diretrizes, políticas, regulamentos, normas e orientações.

## PM-16: Programa de Conscientização sobre Ameaças (P0)

**Descrição do Controle:**A organização implementa um programa de conscientização de ameaças que inclui um recurso de compartilhamento de informações entre organizações.  
  
**Guia Adicional:**Devido à sofisticação constante e crescente dos adversários, especialmente a ameaça persistente avançada (APT), está se tornando mais provável que os adversários possam violar ou comprometer com sucesso os sistemas de informações organizacionais. Uma das melhores técnicas para lidar com essa preocupação é que as organizações compartilhem informações sobre ameaças. Isso pode incluir, por exemplo, compartilhamento de eventos de ameaça (táticas, técnicas e procedimentos) que as organizações tenham experimentado, mitigações que as organizações considerem eficazes contra certos tipos de ameaças, inteligência de ameaças (ou seja, indicações e avisos sobre ameaças que são provável que aconteça). O compartilhamento de informações sobre ameaças pode ser bilateral (por exemplo, cooperativas comerciais do governo, cooperativas governo-governo) ou multilateral (por exemplo, organizações que participam de consórcios de compartilhamento de ameaças). As informações sobre ameaças podem ser altamente sensíveis, exigindo acordos e proteção especiais, ou menos sensíveis e compartilhadas livremente.

# RA - Avaliação de Riscos

## RA-1: Política e Procedimentos de Avaliação de Riscos (P1)

**Descrição do Controle:**A organização:  
  
a. Desenvolve, documenta e dissemina para [Atribuição: pessoal ou funções definidas pela organização]:  
  
1. Uma política de avaliação de riscos que lida com propósito, escopo, funções, responsabilidades, compromisso de gerenciamento, coordenação entre entidades organizacionais e conformidade; e  
  
2. Procedimentos para facilitar a implementação da política de avaliação de riscos e controles de avaliação de riscos associados; e  
  
b. Revisa e atualiza a atual:  
  
1. Política de avaliação de riscos [Atribuição: frequência definida pela organização]; e  
  
2. Procedimentos de avaliação de riscos [Atribuição: frequência definida pela organização].  
  
**Guia Adicional:**Esse controle aborda o estabelecimento de políticas e procedimentos para a implementação efetiva de controles de segurança selecionados e aprimoramentos de controle na família RA. As políticas e procedimentos refletem as leis federais aplicáveis, ordens executivas, diretivas, regulamentos, políticas, normas e diretrizes. Políticas e procedimentos do programa de segurança no nível da organização podem tornar desnecessária a necessidade de políticas e procedimentos específicos do sistema. A política pode ser incluída como parte da política geral de segurança da informação para organizações ou, inversamente, pode ser representada por múltiplas políticas refletindo a natureza complexa de certas organizações. Os procedimentos podem ser estabelecidos para o programa de segurança em geral e para sistemas de informação específicos, se necessário. A estratégia de gerenciamento de risco organizacional é um fator chave no estabelecimento de políticas e procedimentos.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-12 | https://csrc.nist.gov/publications/search?keywords-lg=800-12 |
| Publicação Especial NIST 800-30 | https://csrc.nist.gov/publications/search?keywords-lg=800-30 |
| Publicação Especial NIST 800-100 | https://csrc.nist.gov/publications/search?keywords-lg=800-100 |

## RA-2: Categorização de Segurança (P1)

**Descrição do Controle:**A organização:  
  
a. Categoriza as informações e o sistema de informações de acordo com as leis federais aplicáveis, ordens executivas, diretrizes, políticas, regulamentos, normas e orientações;  
  
b. Documenta os resultados da categorização de segurança (incluindo a justificativa de suporte) no plano de segurança do sistema de informações; e  
  
c. Garante que o funcionário autorizador ou representante designado revise e aprove a decisão de categorização de segurança.  
  
**Guia Adicional:**Os limites de autorização claramente definidos são um pré-requisito para decisões efetivas de categorização de segurança. As categorias de segurança descrevem os possíveis impactos adversos às operações organizacionais, ativos organizacionais e indivíduos, se as informações e sistemas de informações organizacionais forem compostos por uma perda de confidencialidade, integridade ou disponibilidade. As organizações conduzem o processo de categorização de segurança como uma atividade em toda a organização, com o envolvimento de diretores de informação, executivos seniores de segurança da informação, proprietários de sistemas de informações, proprietários de missões / negócios e proprietários / administradores de informações. As organizações também consideram os possíveis impactos adversos para outras organizações e, de acordo com a Lei EUA PATRIOT de 2001 e as Diretivas Presidenciais de Segurança Interna, os potenciais impactos adversos em nível nacional. Os processos de categorização de segurança realizados pelas organizações facilitam o desenvolvimento de inventários de ativos de informações e, juntamente com o CM-8, mapeamentos para componentes específicos do sistema de informações onde as informações são processadas, armazenadas ou transmitidas.

**Referências:**

|  |  |
| --- | --- |
| Publicações de Normas Federais de Processamento de Informações N.199 | http://csrc.nist.gov/publications/PubsFIPS.html#199 |
| Publicação Especial NIST 800-30 | https://csrc.nist.gov/publications/search?keywords-lg=800-30 |
| Publicação Especial NIST 800-39 | https://csrc.nist.gov/publications/search?keywords-lg=800-39 |
| Publicação Especial NIST 800-60 | https://csrc.nist.gov/publications/search?keywords-lg=800-60 |

## RA-3: Avaliação de Risco (P1)

**Descrição do Controle:**A organização:  
  
a. Conduz uma avaliação de risco, incluindo a probabilidade e magnitude do dano, a partir do acesso não autorizado, uso, divulgação, interrupção, modificação ou destruição do sistema de informação e das informações que ele processa, armazena ou transmite;  
  
b. Documenta os resultados da avaliação de risco em [Seleção: plano de segurança; relatório de avaliação de risco; [Cessão: documento definido pela organização]];  
  
c. Revisa os resultados da avaliação de riscos [Tarefa: frequência definida pela organização];  
  
d. Divulga os resultados da avaliação de riscos para [Atribuição: pessoal ou funções definidas pela organização]; e  
  
e. Atualiza a avaliação de riscos [Atribuição: frequência definida pela organização] ou sempre que houver alterações significativas no sistema de informações ou no ambiente de operação (incluindo a identificação de novas ameaças e vulnerabilidades) ou outras condições que possam afetar o estado de segurança do sistema.  
  
**Guia Adicional:**Os limites de autorização claramente definidos são um pré-requisito para avaliações de risco eficazes. As avaliações de risco levam em conta ameaças, vulnerabilidades, probabilidade e impacto para operações e ativos organizacionais, indivíduos, outras organizações e a Nação com base na operação e uso de sistemas de informação. As avaliações de risco também levam em conta o risco de partes externas (por exemplo, prestadores de serviços, prestadores de serviços que operam sistemas de informações em nome da organização, indivíduos acessando sistemas de informações organizacionais, terceirizando entidades). De acordo com a política do OMB e as iniciativas de autenticação eletrônica relacionadas, a autenticação de usuários públicos que acessam sistemas de informações federais também pode ser necessária para proteger informações não públicas ou relacionadas à privacidade. Assim, as avaliações organizacionais de risco também abordam o acesso do público aos sistemas de informação federais. As avaliações de risco (formais ou informais) podem ser conduzidas nas três camadas da hierarquia de gerenciamento de riscos (nível de organização, missão / processos de negócios ou sistema de informações) e em qualquer fase do ciclo de vida de desenvolvimento do sistema. As avaliações de risco também podem ser conduzidas em várias etapas da Estrutura de Gerenciamento de Riscos, incluindo categorização, seleção de controle de segurança, implementação de controle de segurança, avaliação de controle de segurança, autorização do sistema de informações e monitoramento de controle de segurança. O RA-3 é digno de nota, pois o controle deve ser parcialmente implementado antes da implementação de outros controles, a fim de completar as duas primeiras etapas da Estrutura de Gerenciamento de Risco. As avaliações de risco podem desempenhar um papel importante nos processos de seleção de controle de segurança, particularmente durante a aplicação das diretrizes de personalização, que incluem a suplementação de controle de segurança.

**Referências:**

|  |  |
| --- | --- |
| OMB Memorando 04-04 | https://georgewbush-whitehouse.archives.gov/omb/memoranda/fy04/m04-04.pdf |
| Publicação Especial NIST 800-30 | https://csrc.nist.gov/publications/search?keywords-lg=800-30 |
| Publicação Especial NIST 800-39 | https://csrc.nist.gov/publications/search?keywords-lg=800-39 |
| FICAM: Identidade Federal, Credencial e Gerenciamento de Acesso | http://idmanagement.gov |

## RA-4: Atualização de Avaliação de Riscos (P0)

**Descrição do Controle:**[Retirado: Incorporado no RA-3].

## RA-5: Digitalização de Vulnerabilidade (P1)

**Descrição do Controle:**A organização:  
  
a. Verifica vulnerabilidades no sistema de informações e em aplicativos hospedados [Atribuição: frequência definida pela organização e/ou aleatoriamente de acordo com o processo definido pela organização] e quando novas vulnerabilidades que potencialmente afetam o sistema / aplicativos são identificadas e relatadas;  
  
b. Emprega ferramentas e técnicas de varredura de vulnerabilidades que facilitam a interoperabilidade entre ferramentas e automatizam partes do processo de gerenciamento de vulnerabilidades usando padrões para:  
  
1. Enumerar plataformas, falhas de software e configurações inadequadas;  
  
2. Formatação de listas de verificação e procedimentos de teste; e  
  
3. Medir o impacto da vulnerabilidade;  
  
c. Analisa relatórios de varredura de vulnerabilidade e resultados de avaliações de controle de segurança;  
  
d. Corrige vulnerabilidades legítimas [Atribuição: tempos de resposta definidos pela organização] de acordo com uma avaliação organizacional dos riscos; e  
  
e. Compartilha informações obtidas do processo de verificação de vulnerabilidades e avaliações de controle de segurança com [Atribuição: pessoal ou funções definidas pela organização] para ajudar a eliminar vulnerabilidades semelhantes em outros sistemas de informações (por exemplo, deficiências ou deficiências sistêmicas).  
  
**Guia Adicional:**A categorização de segurança dos sistemas de informação orienta a frequência e a abrangência das verificações de vulnerabilidade. As organizações determinam a verificação de vulnerabilidade necessária para todos os componentes do sistema de informações, garantindo que as fontes potenciais de vulnerabilidades, como impressoras, scanners e copiadoras em rede, não sejam negligenciadas. As análises de vulnerabilidade para aplicativos de software personalizados podem exigir abordagens adicionais, como análise estática, análise dinâmica, análise binária ou um híbrido das três abordagens. As organizações podem empregar essas abordagens de análise em uma variedade de ferramentas (por exemplo, scanners de aplicativos baseados na Web, ferramentas de análise estática, analisadores binários) e em revisões de código-fonte. A verificação de vulnerabilidade inclui, por exemplo: (i) verificação de níveis de patch; (ii) varredura de funções, portas, protocolos e serviços que não devem ser acessíveis a usuários ou dispositivos; e (iii) varredura de mecanismos de controle de fluxo de informações configurados incorretamente ou operando incorretamente. As organizações consideram o uso de ferramentas que expressam vulnerabilidades na convenção de nomenclatura Common Vulnerabilities and Exposures (CVE) e que usam a Open Vulnerability Assessment Language (OVAL) para determinar / testar a presença de vulnerabilidades. As fontes sugeridas para informações de vulnerabilidade incluem a listagem da Common Weakness Enumeration (CWE) e o National Vulnerability Database (NVD). Além disso, avaliações de controle de segurança, como exercícios em equipe vermelhos, fornecem outras fontes de possíveis vulnerabilidades para as quais verificar. As organizações também consideram o uso de ferramentas que expressam o impacto da vulnerabilidade pelo Sistema de Pontuação de Vulnerabilidade Comum (CVSS).  
  
**Melhorias do Controle:**

### RA-5(1): Digitalização de Vulnerabilidade | Atualização da Capacidade de Ferramenta

A organização emprega ferramentas de verificação de vulnerabilidades que incluem a capacidade de atualizar rapidamente as vulnerabilidades do sistema de informações a serem verificadas.  
Guia Adicional: As vulnerabilidades a serem verificadas precisam ser prontamente atualizadas à medida que novas vulnerabilidades são descobertas, anunciadas e os métodos de verificação desenvolvidos. Esse processo de atualização ajuda a garantir que as possíveis vulnerabilidades no sistema de informações sejam identificadas e resolvidas o mais rápido possível.

### RA-5(2): Digitalização de Vulnerabilidade | Atualização por Frequência / Antes de Nova Busca / Quando Identificada

A organização atualiza as vulnerabilidades do sistema de informações verificadas [Seleção (uma ou mais): [Atribuição: frequência definida pela organização]; antes de uma nova varredura; quando novas vulnerabilidades são identificadas e relatadas].

### RA-5(3): Digitalização de Vulnerabilidade | Padrão / Profundidade de Cobertura

A organização emprega procedimentos de verificação de vulnerabilidades que podem identificar a abrangência e profundidade da cobertura (ou seja, componentes do sistema de informações verificados e vulnerabilidades verificadas).

### RA-5(4): Digitalização de Vulnerabilidade | Informação Descoberta

A organização determina quais informações sobre o sistema de informações podem ser descobertas pelos adversários e, posteriormente, realiza [Tarefa: ações corretivas definidas pela organização].  
Guia Adicional: Informações detectáveis incluem informações que os adversários poderiam obter sem comprometer ou violar diretamente o sistema de informações, por exemplo, coletando informações que o sistema está expondo ou realizando extensas pesquisas na Web. As ações corretivas podem incluir, por exemplo, notificar o pessoal organizacional apropriado, remover as informações designadas ou alterar o sistema de informações para tornar as informações designadas menos relevantes ou atraentes para os adversários.

### RA-5(5): Digitalização de Vulnerabilidade | Acesso Privilegiado

O sistema de informações implementa a autorização de acesso privilegiado para [Atribuição: componentes do sistema de informações identificadas pela organização] para [Atribuição: atividades de verificação de vulnerabilidades definidas pela organização].  
Guia Adicional: Em certas situações, a natureza da verificação de vulnerabilidades pode ser mais intrusiva ou o componente do sistema de informações que é o assunto da verificação pode conter informações altamente confidenciais. A autorização de acesso privilegiado a componentes selecionados do sistema facilita a verificação de vulnerabilidades mais completa e também protege a natureza sensível dessa verificação.

### RA-5(6): Digitalização de Vulnerabilidade | Análises de Tendência Automatizadas

A organização emprega mecanismos automatizados para comparar os resultados das verificações de vulnerabilidades ao longo do tempo para determinar tendências nas vulnerabilidades do sistema de informação.

### RA-5(7): Digitalização de Vulnerabilidade | Detecção Automatizada e Notificação de Componentes Não Autorizados

[Retirado: Incorporado ao CM-8].

### RA-5(8): Digitalização de Vulnerabilidade | Revisar os Registros de Auditoria Históricos

A organização revisa os registros históricos de auditoria para determinar se uma vulnerabilidade identificada no sistema de informações foi explorada anteriormente.

### RA-5(9): Digitalização de Vulnerabilidade | Ensaios e Análises de Penetração

[Retirado: Incorporado ao CA-8].

### RA-5(10): Digitalização de Vulnerabilidade | Informação Correta da Digitalização

A organização correlaciona a saída das ferramentas de varredura de vulnerabilidades para determinar a presença de vetores de ataque com várias vulnerabilidades / vários saltos.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-40 | https://csrc.nist.gov/publications/search?keywords-lg=800-40 |
| Publicação Especial NIST 800-70 | https://csrc.nist.gov/publications/search?keywords-lg=800-70 |
| Publicação Especial NIST 800-115 | https://csrc.nist.gov/publications/search?keywords-lg=800-115 |
| CWE: Enumeração de Fraqueza Comum | http://cwe.mitre.org |
| NIST - NVD: Banco de Dados Nacional de Vulnerabilidades | http://nvd.nist.gov |

## RA-6: Inquérito à Vigilância Técnica (P0)

**Descrição do Controle:**A organização emprega uma pesquisa de contramedidas de vigilância técnica em [Tarefa: locais definidos pela organização] [Seleção (uma ou mais): [Tarefa: frequência definida pela organização]; [Atribuição: eventos ou indicadores definidos pela organização ocorrem]].  
  
**Guia Adicional:**As pesquisas de contramedidas de vigilância técnica são realizadas por pessoal qualificado para detectar a presença de dispositivos / perigos de vigilância técnica e para identificar deficiências técnicas de segurança que podem ajudar na condução de penetrações técnicas nas instalações pesquisadas. Essas pesquisas fornecem avaliações das posturas de segurança técnica das organizações e instalações e geralmente incluem exames visuais, eletrônicos e físicos completos nas instalações pesquisadas e em torno delas. As pesquisas também fornecem informações úteis para avaliações de risco e exposição organizacional a possíveis adversários.

# CA - Avaliação e Autorização de Segurança

## CA-1: Política e Procedimentos de Avaliação de Segurança e Autorização (P1)

**Descrição do Controle:**A organização:  
  
a. Desenvolve, documenta e divulga para [Atribuição: pessoal ou funções definidas pela organização]:  
  
1. Uma política de avaliação e autorização de segurança que atenda a finalidade, escopo, funções, responsabilidades, compromisso de gerenciamento, coordenação entre entidades organizacionais e conformidade; e  
  
2. Procedimentos para facilitar a implementação da política de avaliação e autorização de segurança e controles associados de avaliação e autorização de segurança; e  
  
b. Revisa e atualiza a atual:  
  
1. Política de avaliação e autorização de segurança [Atribuição: frequência definida pela organização]; e  
  
2. Procedimentos de avaliação e autorização de segurança [Atribuição: frequência definida pela organização].  
  
**Guia Adicional:**Esse controle aborda o estabelecimento de políticas e procedimentos para a implementação efetiva de controles de segurança selecionados e aprimoramentos de controle na família CA. As políticas e procedimentos refletem as leis federais aplicáveis, ordens executivas, diretivas, regulamentos, políticas, normas e diretrizes. Políticas e procedimentos do programa de segurança no nível da organização podem tornar desnecessária a necessidade de políticas e procedimentos específicos do sistema. A política pode ser incluída como parte da política geral de segurança da informação para organizações ou, inversamente, pode ser representada por múltiplas políticas refletindo a natureza complexa de certas organizações. Os procedimentos podem ser estabelecidos para o programa de segurança em geral e para sistemas de informação específicos, se necessário. A estratégia de gerenciamento de risco organizacional é um fator chave no estabelecimento de políticas e procedimentos.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-12 | https://csrc.nist.gov/publications/search?keywords-lg=800-12 |
| Publicação Especial NIST 800-37 | https://csrc.nist.gov/publications/search?keywords-lg=800-37 |
| Publicação Especial NIST 800-53A | https://csrc.nist.gov/publications/search?keywords-lg=800-53A |
| Publicação Especial NIST 800-100 | https://csrc.nist.gov/publications/search?keywords-lg=800-100 |

## CA-2: Avaliações de Segurança (P2)

**Descrição do Controle:**A organização:  
  
a. Desenvolve um plano de avaliação de segurança que descreve o escopo da avaliação, incluindo:  
  
1. Controles de segurança e aprimoramentos de controle em avaliação;  
  
2. Procedimentos de avaliação a serem usados para determinar a eficácia do controle de segurança; e  
  
3. Ambiente de avaliação, equipe de avaliação e funções e responsabilidades de avaliação;  
  
b. Avalia os controles de segurança no sistema de informações e seu ambiente de operação [Atribuição: frequência definida pela organização] para determinar a extensão em que os controles são implementados corretamente, operando conforme o esperado e produzindo o resultado desejado com relação aos requisitos de segurança estabelecidos;  
  
c. Produz um relatório de avaliação de segurança que documenta os resultados da avaliação; e  
  
d. Fornece os resultados da avaliação de controle de segurança para [Atribuição: indivíduos ou funções definidas pela organização].  
  
**Guia Adicional:**As organizações avaliam os controles de segurança nos sistemas de informações organizacionais e nos ambientes em que esses sistemas operam como parte de: (i) autorizações de segurança iniciais e contínuas; (ii) avaliações anuais do FISMA; (iii) monitoramento contínuo; e (iv) atividades do ciclo de vida de desenvolvimento do sistema. Avaliações de segurança: (i) garantir que a segurança das informações seja incorporada aos sistemas de informações organizacionais; (ii) identificar pontos fracos e deficiências no início do processo de desenvolvimento; (iii) fornecer informações essenciais necessárias para tomar decisões baseadas em riscos como parte dos processos de autorização de segurança; e (iv) garantir a conformidade com os procedimentos de mitigação de vulnerabilidades. As avaliações são realizadas nos controles de segurança implementados no Apêndice F (catálogo principal) e Apêndice G (controles de Gerenciamento de Programas), conforme documentado nos Planos de Segurança do Sistema e nos Planos de Programas de Segurança da Informação. As organizações podem usar outros tipos de atividades de avaliação, como varredura de vulnerabilidades e monitoramento do sistema, para manter a postura de segurança dos sistemas de informação durante todo o ciclo de vida. Os relatórios de avaliação de segurança documentam os resultados da avaliação em detalhes suficientes, conforme necessário pelas organizações, para determinar a precisão e a integridade dos relatórios e se os controles de segurança são implementados corretamente, operando conforme o planejado e produzindo o resultado desejado com relação ao cumprimento dos requisitos de segurança. O requisito do FISMA para avaliar os controles de segurança pelo menos anualmente não requer atividades de avaliação adicionais às atividades já implementadas nos processos de autorização de segurança organizacional. Os resultados da avaliação de segurança são fornecidos às pessoas ou funções apropriadas para os tipos de avaliação que estão sendo conduzidas. Por exemplo, avaliações conduzidas em apoio a decisões de autorização de segurança são fornecidas aos oficiais autorizadores ou representantes oficiais designados. Para satisfazer os requisitos de avaliação anual, as organizações podem usar os resultados da avaliação das seguintes fontes: (i) autorizações iniciais ou em andamento do sistema de informações; (ii) monitoramento contínuo; ou (iii) atividades do ciclo de vida de desenvolvimento do sistema. As organizações garantem que os resultados da avaliação de segurança sejam atuais, relevantes para a determinação da eficácia do controle de segurança e sejam obtidos com o nível apropriado de independência do avaliador. Os resultados existentes da avaliação de controle de segurança podem ser reutilizados na medida em que os resultados ainda são válidos e também podem ser complementados com avaliações adicionais, conforme necessário. Após as autorizações iniciais e de acordo com a política do OMB, as organizações avaliam os controles de segurança durante o monitoramento contínuo. As organizações estabelecem a frequência das avaliações contínuas do controle de segurança, de acordo com as estratégias organizacionais de monitoramento contínuo. Os alertas de vulnerabilidade de garantia de informações fornecem exemplos úteis de procedimentos de mitigação de vulnerabilidades. Auditorias externas (por exemplo, auditorias de entidades externas, como agências reguladoras) estão fora do escopo deste controle.  
  
**Melhorias do Controle:**

### CA-2(1): Avaliações de Segurança | Assessores Independentes

A organização emprega avaliadores ou equipes de avaliação com [Atribuição: nível de independência definido pela organização] para realizar avaliações de controle de segurança.  
Guia Adicional: Avaliadores independentes ou equipes de avaliação são indivíduos ou grupos que conduzem avaliações imparciais dos sistemas de informações organizacionais. A imparcialidade implica que os avaliadores estejam livres de quaisquer conflitos de interesse percebidos ou reais com relação ao desenvolvimento, operação ou gerenciamento dos sistemas de informações organizacionais em avaliação ou à determinação da eficácia do controle de segurança. Para obter imparcialidade, os avaliadores não devem: (i) criar um interesse mútuo ou conflitante com as organizações onde as avaliações estão sendo conduzidas; (ii) avaliar seu próprio trabalho; (iii) atuar como gerentes ou funcionários das organizações que estão servindo; ou (iv) colocar-se em posições de advocacia para as organizações que adquirem seus serviços. Avaliações independentes podem ser obtidas a partir de elementos dentro das organizações ou podem ser contratadas para entidades do setor público ou privado fora das organizações. Os oficiais de autorização determinam o nível de independência necessário com base nas categorias de segurança dos sistemas de informação e/ou no risco final para operações organizacionais, ativos organizacionais ou indivíduos. As autoridades autorizadoras também determinam se o nível de independência do avaliador fornece garantia suficiente de que os resultados são sólidos e podem ser usados para tomar decisões credíveis e baseadas no risco. Isso inclui determinar se os serviços de avaliação de segurança contratados têm independência suficiente, por exemplo, quando os proprietários do sistema de informações não estão diretamente envolvidos nos processos de contratação ou não podem influenciar indevidamente a imparcialidade dos avaliadores que realizam as avaliações. Em situações especiais, por exemplo, quando as organizações que possuem os sistemas de informação são pequenas ou as estruturas organizacionais exigem que as avaliações sejam conduzidas por indivíduos que estão na cadeia de desenvolvimento, operacional ou de gerenciamento dos proprietários de sistemas, a independência nos processos de avaliação pode ser alcançada, garantindo que os resultados da avaliação sejam cuidadosamente revisados e analisados por equipes independentes de especialistas para validar a integridade, precisão, integridade e confiabilidade dos resultados. As organizações reconhecem que as avaliações realizadas para outros fins que não o apoio direto às decisões de autorização são, quando realizadas por avaliadores com independência suficiente, mais suscetíveis de serem utilizáveis para tais decisões, reduzindo assim a necessidade de repetir avaliações.

### CA-2(2): Avaliações de Segurança | Avaliações Especializadas

A organização inclui, como parte das avaliações de controle de segurança, [Atribuição: frequência definida pela organização], [Seleção: anunciada; sem aviso prévio], [Seleção (um ou mais): monitoramento aprofundado; verificação de vulnerabilidades; teste de usuário malicioso; avaliação de ameaças internas; teste de desempenho / carga; [Tarefa: outras formas de avaliação de segurança definidas pela organização]].  
Guia Adicional: As organizações podem empregar monitoramento do sistema de informações, avaliações de ameaças internas, testes de usuários mal-intencionados e outras formas de testes (por exemplo, verificação e validação) para melhorar a prontidão, exercitando os recursos organizacionais e indicando os níveis atuais de desempenho como um meio de concentrar ações para melhorar a segurança. As organizações realizam atividades de avaliação de acordo com as leis federais aplicáveis, ordens executivas, diretrizes, políticas, regulamentos e normas. Autoridades autorizadas aprovam os métodos de avaliação em coordenação com a função executiva de risco organizacional. As organizações podem incorporar vulnerabilidades descobertas durante as avaliações nos processos de correção de vulnerabilidades.

### CA-2(3): Avaliações de Segurança | Organizações Externas

A organização aceita os resultados de uma avaliação de [Atribuição: sistema de informações definido pela organização] realizada por [Atribuição: organização externa definida pela organização] quando a avaliação atende a [Atribuição: requisitos definidos pela organização].  
Guia Adicional: As organizações geralmente podem confiar em avaliações de sistemas de informações específicos por outras organizações (externas). A utilização dessas avaliações existentes (ou seja, a reutilização de evidências de avaliação existentes) pode diminuir significativamente o tempo e os recursos necessários para as avaliações organizacionais, limitando a quantidade de atividades de avaliação independentes que as organizações precisam realizar. Os fatores que as organizações podem considerar para determinar se devem aceitar os resultados da avaliação de organizações externas podem variar. As determinações para aceitação dos resultados da avaliação podem ser baseadas, por exemplo, em experiências anteriores de avaliação que uma organização teve com outra organização, na reputação que as organizações têm em relação a avaliações, no nível de detalhe da documentação de avaliação fornecida ou nos mandatos impostos às organizações por legislação, políticas ou diretrizes federais.

**Referências:**

|  |  |
| --- | --- |
| Ordem Executiva da Casa Branca Nº13587 | http://www.whitehouse.gov/the-press-office/2011/10/07/executive-order-13587-structural-reforms-improve-security-classified-net |
| Publicações de Normas Federais de Processamento de Informações N.199 | http://csrc.nist.gov/publications/PubsFIPS.html#199 |
| Publicação Especial NIST 800-37 | https://csrc.nist.gov/publications/search?keywords-lg=800-37 |
| Publicação Especial NIST 800-39 | https://csrc.nist.gov/publications/search?keywords-lg=800-39 |
| Publicação Especial NIST 800-53A | https://csrc.nist.gov/publications/search?keywords-lg=800-53A |
| Publicação Especial NIST 800-115 | https://csrc.nist.gov/publications/search?keywords-lg=800-115 |
| Publicação Especial NIST 800-137 | https://csrc.nist.gov/publications/search?keywords-lg=800-137 |

## CA-3: Interconexões do Sistema (P1)

**Descrição do Controle:**A organização:  
  
a. Autoriza conexões do sistema de informação com outros sistemas de informação através do uso de Acordos de Segurança de Interconexão;  
  
b. Documentos, para cada interconexão, as características da interface, os requisitos de segurança e a natureza das informações comunicadas; e  
  
c. Revisa e atualiza os acordos de segurança de interconexão [atribuição: frequência definida pela organização].  
  
**Guia Adicional:**Esse controle aplica-se a conexões dedicadas entre sistemas de informações (ou seja, interconexões do sistema) e não se aplica a conexões transitórias controladas pelo usuário, como e-mail e navegação no site. As organizações consideram cuidadosamente os riscos que podem ser introduzidos quando os sistemas de informação estão conectados a outros sistemas com diferentes requisitos de segurança e controles de segurança, tanto dentro das organizações quanto externos às organizações. Os gestores orçamentais determinam o risco associado às conexões do sistema de informação e aos controles apropriados empregados. Se os sistemas de interconexão tiverem o mesmo oficial autorizador, as organizações não precisam desenvolver Acordos de Segurança de Interconexão. Em vez disso, as organizações podem descrever as características da interface entre esses sistemas de interconexão em seus respectivos planos de segurança. Se os sistemas de interconexão tiverem diferentes autoridades autorizadoras na mesma organização, as organizações poderão desenvolver Contratos de Segurança de Interconexão ou descrever as características da interface entre sistemas nos planos de segurança dos respectivos sistemas. As organizações também podem incorporar informações do Contrato de Segurança da Interconexão em contratos formais, especialmente para interconexões estabelecidas entre agências federais e organizações não federais (por exemplo, setor privado). As considerações de risco também incluem sistemas de informação que compartilham as mesmas redes. Para certas tecnologias (por exemplo, espaço, veículos aéreos não tripulados e dispositivos médicos), pode haver conexões especializadas em vigor durante os testes pré-operacionais. Tais conexões podem exigir Acordos de Segurança de Interconexão e estão sujeitas a controles de segurança adicionais.  
  
**Melhorias do Controle:**

### CA-3(1): Interconexões do Sistema | Ligações de Sistema Nacional de Segurança Não Classificadas

A organização proíbe a conexão direta de um [Cessão: sistema de segurança nacional não classificado e definido pela organização] a uma rede externa sem o uso de [Cessão: dispositivo de proteção de limite definido pela organização].  
Guia Adicional: As organizações normalmente não têm controle sobre redes externas (por exemplo, a Internet). Os dispositivos de proteção de limite aprovados (por exemplo, roteadores, firewalls) mediam as comunicações (ou seja, fluxos de informações) entre sistemas de segurança nacional não classificados e redes externas. Esse aprimoramento de controle é necessário para organizações que processam, armazenam ou transmitem Informações Não Classificadas Controladas (CUI).

### CA-3(2): Interconexões do Sistema | Ligações de Sistema Nacional de Segurança Classificadas

A organização proíbe a conexão direta de um sistema de segurança nacional classificado a uma rede externa sem o uso de [Atribuição: dispositivo de proteção de limite definido pela organização].  
Guia Adicional: As organizações normalmente não têm controle sobre redes externas (por exemplo, a Internet). Os dispositivos de proteção de limites aprovados (por exemplo, roteadores, firewalls) mediam as comunicações (ou seja, fluxos de informações) entre sistemas de segurança nacional classificados e redes externas. Além disso, os dispositivos de proteção de limite aprovados (sistemas de interface / domínio cruzado geralmente gerenciados) fornecem imposição do fluxo de informações dos sistemas de informação às redes externas.

### CA-3(3): Interconexões do Sistema | Ligações de Sistema de Segurança Não Nacional Não Classificadas

A organização proíbe a conexão direta de um [Cessão: sistema de segurança não nacional não classificado e definido pela organização] a uma rede externa sem o uso de [Cessão; dispositivo de proteção de limites definido pela organização].  
Guia Adicional: As organizações normalmente não têm controle sobre redes externas (por exemplo, a Internet). Os dispositivos de proteção de limites aprovados (por exemplo, roteadores, firewalls) mediam as comunicações (ou seja, fluxos de informações) entre sistemas de segurança não nacionais não classificados e redes externas. Esse aprimoramento de controle é necessário para organizações que processam, armazenam ou transmitem Informações Não Classificadas Controladas (CUI).

### CA-3(4): Interconexões do Sistema | Conexões com Redes Públicas

A organização proíbe a conexão direta de um [Trabalho: sistema de informações definido pela organização] a uma rede pública.  
Guia Adicional: Uma rede pública é qualquer rede acessível ao público em geral, incluindo, por exemplo, a Internet e extranets organizacionais com acesso público.

### CA-3(5): Interconexões do Sistema | Restrições à Conexão de Sistemas Externos

A organização emprega [Seleção: permitir tudo, negar por exceção; política de negar tudo, permitir por exceção], para permitir que [Atribuição: sistemas de informação definidos pela organização] se conecte a sistemas de informação externos.  
Guia Adicional: As organizações podem restringir a conectividade do sistema de informações a domínios externos (por exemplo, sites) empregando uma das duas políticas relacionadas a essa conectividade: (i) permitir tudo, negar por exceção, também conhecida como lista negra (a mais fraca das duas políticas); ou (ii) negar tudo, permitir por exceção, também conhecida como lista de permissões (a mais forte das duas políticas). Para qualquer política, as organizações determinam quais exceções, se houver, são aceitáveis.

**Referências:**

|  |  |
| --- | --- |
| Publicações de Normas Federais de Processamento de Informações N.199 | http://csrc.nist.gov/publications/PubsFIPS.html#199 |
| Publicação Especial NIST 800-47 | https://csrc.nist.gov/publications/search?keywords-lg=800-47 |

## CA-4: Certificação de Segurança (P0)

**Descrição do Controle:**[Retirado: Incorporado ao CA-2].

## CA-5: Plano de Ação e Marcos (P3)

**Descrição do Controle:**A organização:  
  
a. Desenvolve um plano de ação e marcos para o sistema de informação documentar as ações corretivas planejadas da organização para corrigir deficiências ou deficiências observadas durante a avaliação dos controles de segurança e reduzir ou eliminar vulnerabilidades conhecidas no sistema; e  
  
b. Atualiza o plano de ação e os marcos existentes [Atribuição: frequência definida pela organização] com base nas descobertas das avaliações de controles de segurança, análises de impacto na segurança e atividades de monitoramento contínuo.  
  
**Guia Adicional:**Os planos de ação e os marcos são documentos importantes nos pacotes de autorização de segurança e estão sujeitos aos requisitos de relatórios federais estabelecidos pelo OMB.  
  
**Melhorias do Controle:**

### CA-5(1): Plano de Ação e Marcos | Suporte de Automação para Precisão

A organização emprega mecanismos automatizados para ajudar a garantir que o plano de ação e os marcos do sistema de informações sejam precisos, atualizados e prontamente disponíveis.

**Referências:**

|  |  |
| --- | --- |
| OMB Memorando 02-01 | https://georgewbush-whitehouse.archives.gov/omb/memoranda/m02-01.html |
| Publicação Especial NIST 800-37 | https://csrc.nist.gov/publications/search?keywords-lg=800-37 |

## CA-6: Autorização de Segurança (P2)

**Descrição do Controle:**A organização:  
  
a. Designa um executivo ou gerente de nível sênior como o funcionário autorizador do sistema de informação;  
  
b. Garante que o gestor orçamental autorize o sistema de informação a processar antes de iniciar as operações; e  
  
c. Atualiza a autorização de segurança [Atribuição: frequência definida pela organização].  
  
**Guia Adicional:**Autorizações de segurança são decisões de gerenciamento oficiais, transmitidas por meio de documentos de decisão de autorização, por altos funcionários ou executivos organizacionais (ou seja, oficiais autorizadores) para autorizar a operação de sistemas de informação e aceitar explicitamente o risco para operações e ativos organizacionais, indivíduos, outras organizações e Nação baseada na implementação de controles de segurança acordados. As autoridades autorizadoras supervisionam o orçamento dos sistemas de informações organizacionais ou assumem a responsabilidade pelas operações de missão / negócios suportados por esses sistemas. O processo de autorização de segurança é uma responsabilidade inerentemente federal e, portanto, os funcionários responsáveis pela autorização devem ser funcionários federais. Por meio do processo de autorização de segurança, os funcionários responsáveis pela autorização assumem a responsabilidade e são responsáveis pelos riscos de segurança associados à operação e uso dos sistemas de informações organizacionais. Consequentemente, os funcionários responsáveis pela autorização estão em posições com níveis de autoridade compatíveis com a compreensão e aceitação desses riscos relacionados à segurança da informação. A política OMB exige que as organizações realizem autorizações contínuas de sistemas de informação implementando programas de monitoramento contínuo. Os programas de monitoramento contínuo podem atender aos requisitos de reautorização de três anos, portanto, processos separados de reautorização não são necessários. Por meio do emprego de processos abrangentes de monitoramento contínuo, as informações críticas contidas nos pacotes de autorização (ou seja, planos de segurança, relatórios de avaliação de segurança e planos de ação e marcos) são atualizadas continuamente, fornecendo às autoridades autorizadas e aos proprietários de sistemas de informação uma atualização status atualizado do estado de segurança dos sistemas de informações organizacionais e ambientes de operação. Para reduzir o custo administrativo da reautorização da segurança, as autoridades autorizadoras usam os resultados dos processos de monitoramento contínuo ao máximo possível como base para a tomada de decisões de reautorização.

**Referências:**

|  |  |
| --- | --- |
| OMB Circular A-130 | https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf |
| OMB Memorando 11-33 | https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2011/m11-33.pdf |
| Publicação Especial NIST 800-37 | https://csrc.nist.gov/publications/search?keywords-lg=800-37 |
| Publicação Especial NIST 800-137 | https://csrc.nist.gov/publications/search?keywords-lg=800-137 |

## CA-7: Monitoramento Contínuo (P2)

**Descrição do Controle:**A organização desenvolve uma estratégia de monitoramento contínuo e implementa um programa de monitoramento contínuo que inclui:  
  
a. Estabelecimento de [atribuição: métricas definidas pela organização] a ser monitorado;  
  
b. Estabelecimento de [Designação: frequências definidas pela organização] para monitoramento e [Designação: frequências definidas pela organização] para avaliações que apoiam esse monitoramento;  
  
c. Avaliações de controle de segurança em andamento de acordo com a estratégia de monitoramento contínuo organizacional;  
  
d. Monitoramento contínuo do status de segurança das métricas definidas pela organização, de acordo com a estratégia de monitoramento contínuo organizacional;  
  
e. Correlação e análise de informações relacionadas à segurança geradas por avaliações e monitoramento;  
  
f. Ações de resposta para abordar resultados da análise de informações relacionadas à segurança; e  
  
g. Relatar o status de segurança da organização e o sistema de informações a [Atribuição: pessoal ou funções definidas pela organização] [Atribuição: frequência definida pela organização].  
  
**Guia Adicional:**Os programas de monitoramento contínuo facilitam o conhecimento contínuo de ameaças, vulnerabilidades e segurança da informação para apoiar as decisões de gerenciamento de riscos organizacionais. Os termos contínuo e contínuo implicam que as organizações avaliem / analisem os controles de segurança e os riscos relacionados à segurança da informação com uma frequência suficiente para apoiar as decisões baseadas em risco organizacional. Os resultados dos programas de monitoramento contínuo geram ações apropriadas de resposta a riscos pelas organizações. Os programas de monitoramento contínuo também permitem que as organizações mantenham as autorizações de segurança de sistemas de informação e controles comuns ao longo do tempo em ambientes altamente dinâmicos de operação, com mudanças nas necessidades de missão / negócios, ameaças, vulnerabilidades e tecnologias. O acesso contínuo às informações relacionadas à segurança por meio de relatórios / painéis oferece aos funcionários da organização a capacidade de tomar decisões de gerenciamento de risco mais efetivas e oportunas, incluindo decisões contínuas de autorização de segurança. A automação suporta atualizações mais frequentes de pacotes de autorização de segurança, inventários de hardware / software / firmware e outras informações do sistema. A eficácia é aprimorada ainda mais quando as saídas de monitoramento contínuo são formatadas para fornecer informações específicas, mensuráveis, acionáveis, relevantes e oportunas. As atividades de monitoramento contínuo são dimensionadas de acordo com as categorias de segurança dos sistemas de informação.  
  
**Melhorias do Controle:**

### CA-7(1): Monitoramento Contínuo | Avaliação Independente

A organização emprega avaliadores ou equipes de avaliação com [Atribuição: nível de independência definido pela organização] para monitorar os controles de segurança no sistema de informações continuamente.  
Guia Adicional: As organizações podem maximizar o valor das avaliações dos controles de segurança durante o processo de monitoramento contínuo, exigindo que essas avaliações sejam conduzidas por avaliadores ou equipes de avaliação com níveis adequados de independência, com base em estratégias de monitoramento contínuo. A independência do avaliador fornece um certo grau de imparcialidade ao processo de monitoramento. Para alcançar tal imparcialidade, os avaliadores não devem: (i) criar um interesse mútuo ou conflitante com as organizações onde as avaliações estão sendo conduzidas; (ii) avaliar seu próprio trabalho; (iii) atuar como gerentes ou funcionários das organizações que estão servindo; ou (iv) colocar-se em posições de advocacia para as organizações que adquirem seus serviços.

### CA-7(2): Monitoramento Contínuo | Tipos de Avaliações

[Retirado: Incorporado ao CA-2].

### CA-7(3): Monitoramento Contínuo | Análises de Tendência

A organização emprega análises de tendências para determinar se as implementações de controle de segurança, a frequência das atividades de monitoramento contínuo e/ou os tipos de atividades usadas no processo de monitoramento contínuo precisam ser modificadas com base em dados empíricos.  
Guia Adicional: As análises de tendências podem incluir, por exemplo, o exame de informações recentes sobre ameaças relacionadas aos tipos de eventos de ameaças que ocorreram na organização ou no governo federal, taxas de sucesso de certos tipos de ataques cibernéticos, vulnerabilidades emergentes nas tecnologias da informação, técnicas de engenharia social em evolução, resultados de várias avaliações de controle de segurança, a eficácia das definições de configuração e as conclusões dos Inspetores-Gerais ou auditores.

**Referências:**

|  |  |
| --- | --- |
| OMB Memorando 11-33 | https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2011/m11-33.pdf |
| Publicação Especial NIST 800-37 | https://csrc.nist.gov/publications/search?keywords-lg=800-37 |
| Publicação Especial NIST 800-39 | https://csrc.nist.gov/publications/search?keywords-lg=800-39 |
| Publicação Especial NIST 800-53A | https://csrc.nist.gov/publications/search?keywords-lg=800-53A |
| Publicação Especial NIST 800-115 | https://csrc.nist.gov/publications/search?keywords-lg=800-115 |
| Publicação Especial NIST 800-137 | https://csrc.nist.gov/publications/search?keywords-lg=800-137 |
| US-CERT - Alertas Técnicos de Segurança Cibernética | http://www.us-cert.gov/ncas/alerts |

## CA-8: Treinamento de Invasão (PenTest) (P2)

**Descrição do Controle:**A organização realiza teste de penetração [Atribuição: frequência definida pela organização] em [Atribuição: sistemas de informação definidos pela organização ou componentes do sistema].  
  
**Guia Adicional:**O teste de penetração é um tipo especializado de avaliação realizada em sistemas de informação ou componentes individuais do sistema para identificar vulnerabilidades que podem ser exploradas por adversários. Esses testes podem ser usados para validar vulnerabilidades ou determinar o grau de resistência que os sistemas de informações organizacionais têm dos adversários dentro de um conjunto de restrições especificadas (por exemplo, tempo, recursos e/ou habilidades). O teste de penetração tenta duplicar as ações dos adversários na realização de ataques cibernéticos hostis contra organizações e fornece uma análise mais profunda das fraquezas / deficiências relacionadas à segurança. As organizações também podem usar os resultados das análises de vulnerabilidade para apoiar atividades de teste de penetração. O teste de penetração pode ser realizado nos componentes de hardware, software ou firmware de um sistema de informações e pode exercer controles de segurança físicos e técnicos. Um método padrão para teste de penetração inclui, por exemplo: (i) análise de pré-teste com base no conhecimento completo do sistema de destino; (ii) identificação pré-teste de vulnerabilidades potenciais com base na análise pré-teste; e (iii) testes projetados para determinar a capacidade de exploração das vulnerabilidades identificadas. Todas as partes concordam com as regras de contratação antes do início dos cenários de teste de penetração. As organizações correlacionam as regras de participação dos testes de penetração com as ferramentas, técnicas e procedimentos previstos para serem empregados pelos adversários que executam ataques. As avaliações de riscos organizacionais orientam as decisões sobre o nível de independência necessário para o pessoal que realiza os testes de penetração.  
  
**Melhorias do Controle:**

### CA-8(1): Treinamento de Invasão (PenTest) | Agente ou Equipe de Penetração Independente

A organização emprega um agente ou equipe de penetração independente para realizar testes de penetração no sistema de informações ou nos componentes do sistema.  
Guia Adicional: Agentes ou equipes independentes de penetração são indivíduos ou grupos que realizam testes imparciais de penetração nos sistemas de informações organizacionais. A imparcialidade implica que os agentes ou equipes de penetração estejam livres de quaisquer conflitos de interesse percebidos ou reais em relação ao desenvolvimento, operação ou gerenciamento dos sistemas de informação que são os alvos dos testes de penetração. As orientações suplementares para CA-2 (1) fornecem informações adicionais sobre avaliações independentes que podem ser aplicadas ao teste de penetração.

### CA-8(2): Treinamento de Invasão (PenTest) | Exercícios de Equipe Vermelha (Red Team)

A organização emprega [Atribuição: exercícios de equipe vermelhos definidos pela organização] para simular tentativas dos adversários de comprometer os sistemas de informações organizacionais de acordo com [Atribuição: regras de engajamento definidas pela organização].  
Guia Adicional: Os exercícios da equipe vermelha estendem os objetivos do teste de penetração, examinando a postura de segurança das organizações e sua capacidade de implementar defesas cibernéticas eficazes. Dessa forma, os exercícios em equipe vermelhos refletem tentativas contraditórias simuladas de comprometer as funções da missão / negócios da organização e fornecem uma avaliação abrangente do estado de segurança dos sistemas e organizações de informação. Tentativas contraditórias simuladas de comprometer missões organizacionais / funções de negócios e os sistemas de informações que as suportam podem incluir ataques focados na tecnologia (por exemplo, interações com hardware, software ou componentes de firmware e/ou processos de missão / negócios) e engenharia social - ataques baseados em dados (por exemplo, interações por e-mail, telefone, navegação no ombro ou conversas pessoais). Embora os testes de penetração possam ser amplamente baseados em laboratório, as organizações usam exercícios em equipe vermelhos para fornecer avaliações mais abrangentes que refletem as condições do mundo real. Os exercícios em equipe vermelhos podem ser usados para aprimorar o conhecimento e o treinamento em segurança e avaliar os níveis de eficácia do controle de segurança.

## CA-9: Conexões do Sistema Interno (P2)

**Descrição do Controle:**A organização:  
  
a. Autoriza conexões internas de [Atribuição: componentes do sistema de informação definido pela organização ou classes de componentes] ao sistema de informação; e  
  
b. Documentos, para cada conexão interna, as características da interface, os requisitos de segurança e a natureza das informações comunicadas.  
  
**Guia Adicional:**Esse controle se aplica a conexões entre sistemas de informações organizacionais e componentes (separados) do sistema constituinte (ou seja, conexões dentro do sistema), incluindo, por exemplo, conexões do sistema com dispositivos móveis, notebooks / computadores de mesa, impressoras, copiadoras, fac-símiles, scanners, sensores e servidores. Em vez de autorizar cada conexão interna individual, as organizações podem autorizar conexões internas para uma classe de componentes com características e/ou configurações comuns, por exemplo, todas as impressoras digitais, scanners e copiadoras com capacidade especificada de processamento, armazenamento e transmissão ou todos os dispositivos inteligentes. telefones com uma configuração de linha de base específica.  
  
**Melhorias do Controle:**

### CA-9(1): Conexões do Sistema Interno | Verificações de Conformidade com a Segurança

O sistema de informações executa verificações de conformidade de segurança nos componentes constituintes do sistema antes do estabelecimento da conexão interna.  
Guia Adicional: As verificações de conformidade de segurança podem incluir, por exemplo, verificação da configuração da linha de base relevante.

# SC - Proteção de Sistemas e Comunicações

## SC-1: Política e Procedimentos de Proteção de Sistemas e Comunicações (P1)

**Descrição do Controle:**A organização:  
  
a. Desenvolve, documenta e divulga para [Atribuição: pessoal ou funções definidas pela organização]:  
  
1. Uma política de proteção de sistemas e comunicações que aborde objetivos, escopo, funções, responsabilidades, comprometimento gerencial, coordenação entre entidades organizacionais e conformidade; e  
  
2. Procedimentos para facilitar a implementação da política de proteção do sistema e das comunicações e dos controles associados ao sistema e da proteção das comunicações; e  
  
b. Analisa e atualiza a atual:  
  
1. Política de proteção de sistemas e comunicações [Atribuição: frequência definida pela organização]; e  
  
2. Procedimentos de proteção de sistemas e comunicações [Atribuição: frequência definida pela organização].  
  
**Guia Adicional:**Esse controle trata do estabelecimento de políticas e procedimentos para a implementação efetiva de controles de segurança selecionados e aprimoramentos de controle na família SC. As políticas e procedimentos refletem as leis federais aplicáveis, ordens executivas, diretivas, regulamentos, políticas, normas e diretrizes. Políticas e procedimentos do programa de segurança no nível da organização podem tornar desnecessária a necessidade de políticas e procedimentos específicos do sistema. A política pode ser incluída como parte da política geral de segurança da informação para organizações ou, inversamente, pode ser representada por múltiplas políticas refletindo a natureza complexa de certas organizações. Os procedimentos podem ser estabelecidos para o programa de segurança em geral e para sistemas de informação específicos, se necessário. A estratégia de gerenciamento de risco organizacional é um fator chave no estabelecimento de políticas e procedimentos.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-12 | https://csrc.nist.gov/publications/search?keywords-lg=800-12 |
| Publicação Especial NIST 800-100 | https://csrc.nist.gov/publications/search?keywords-lg=800-100 |

## SC-2: Particionamento do Aplicativo (P1)

**Descrição do Controle:**O sistema de informações separa a funcionalidade do usuário (incluindo os serviços de interface do usuário) da funcionalidade de gerenciamento do sistema de informações.  
  
**Guia Adicional:**A funcionalidade de gerenciamento do sistema de informações inclui, por exemplo, funções necessárias para administrar bancos de dados, componentes de rede, estações de trabalho ou servidores e, normalmente, requer acesso privilegiado ao usuário. A separação da funcionalidade do usuário da funcionalidade de gerenciamento do sistema de informações é física ou lógica. As organizações implementam a separação da funcionalidade relacionada ao gerenciamento do sistema da funcionalidade do usuário usando computadores diferentes, unidades de processamento central diferentes, instâncias diferentes de sistemas operacionais, endereços de rede diferentes, técnicas de virtualização ou combinações desses ou de outros métodos, conforme apropriado. Esse tipo de separação inclui, por exemplo, interfaces administrativas da web que usam métodos de autenticação separados para usuários de quaisquer outros recursos do sistema de informações. A separação da funcionalidade do sistema e do usuário pode incluir o isolamento de interfaces administrativas em diferentes domínios e com controles de acesso adicionais.  
  
**Melhorias do Controle:**

### SC-2(1): Particionamento do Aplicativo | Interfaces para Usuários Não Privilegiados

O sistema de informações impede a apresentação da funcionalidade relacionada ao gerenciamento do sistema de informações em uma interface para usuários não privilegiados.  
Guia Adicional: Esse aprimoramento de controle garante que as opções de administração (por exemplo, privilégios de administrador) não estejam disponíveis para usuários em geral (incluindo a proibição do uso da opção de desabilitação comumente usada para eliminar a acessibilidade a essas informações). Tais restrições incluem, por exemplo, não apresentar opções de administração até que os usuários estabeleçam sessões com privilégios de administrador.

## SC-3: Isolamento das Funções de Segurança (P1)

**Descrição do Controle:**O sistema de informações isola funções de segurança de funções não seguras.  
  
**Guia Adicional:**O sistema de informações isola funções de segurança de funções não seguras por meio de um limite de isolamento (implementado via partições e domínios). Esse isolamento controla o acesso e protege a integridade do hardware, software e firmware que executam essas funções de segurança. Os sistemas de informação implementam a separação de código (isto é, separação de funções de segurança de funções não seguras) de várias maneiras, incluindo, por exemplo, o fornecimento de kernels de segurança por meio de anéis ou modos de processador. Para código que não é do kernel, o isolamento da função de segurança geralmente é alcançado por meio de proteções do sistema de arquivos que servem para proteger o código no disco e proteções do espaço de endereço que protegem a execução do código. Os sistemas de informação restringem o acesso às funções de segurança através do uso de mecanismos de controle de acesso e da implementação de recursos com menos privilégios. Embora o ideal seja que todo o código dentro do limite de isolamento da função de segurança contenha apenas código relevante para segurança, às vezes é necessário incluir funções de não segurança dentro do limite de isolamento como uma exceção.  
  
**Melhorias do Controle:**

### SC-3(1): Isolamento das Funções de Segurança | Separação de Hardware

O sistema de informações utiliza mecanismos subjacentes de separação de hardware para implementar o isolamento das funções de segurança.  
Guia Adicional: Os mecanismos subjacentes de separação de hardware incluem, por exemplo, arquiteturas de anel de hardware, comumente implementadas em microprocessadores, e segmentação de endereço imposta por hardware usada para suportar objetos de armazenamento logicamente distintos com atributos separados (isto é, legíveis, graváveis).

### SC-3(2): Isolamento das Funções de Segurança | Funções de Controle de Acesso / Fluxo

O sistema de informações isola as funções de segurança que impõem controle de acesso e fluxo de informações de funções não seguras e de outras funções de segurança.  
Guia Adicional: O isolamento da função de segurança ocorre como resultado da implementação; as funções ainda podem ser digitalizadas e monitoradas. As funções de segurança potencialmente isoladas das funções de controle de acesso e controle de fluxo incluem, por exemplo, funções de auditoria, detecção de intrusões e antivírus.

### SC-3(3): Isolamento das Funções de Segurança | Minimizar Funcionalidades que Não são de Segurança

A organização minimiza o número de funções de não segurança incluídas no limite de isolamento que contém funções de segurança.  
Guia Adicional: Nos casos em que não é possível obter um estrito isolamento das funções de não segurança das funções de segurança, é necessário executar ações para minimizar as funções relevantes não relacionadas à segurança dentro do limite da função de segurança. As funções de não segurança contidas dentro do limite de isolamento são consideradas relevantes para a segurança, porque erros ou mal-intencionados em tal software, em virtude de estarem dentro do limite, podem afetar as funções de segurança dos sistemas de informações organizacionais. O objetivo do projeto é que as partes específicas dos sistemas de informações que fornecem segurança das informações sejam de tamanho / complexidade mínimos. Minimizar o número de funções de não segurança nos componentes de sistemas de informações relevantes para a segurança permite que os designers e implementadores concentrem-se apenas nas funções necessárias para fornecer a capacidade de segurança desejada (geralmente a imposição de acesso). Ao minimizar as funções de não segurança dentro dos limites de isolamento, a quantidade de código que deve ser confiável para impor políticas de segurança é reduzida, contribuindo assim para a compreensibilidade.

### SC-3(4): Isolamento das Funções de Segurança | Acoplamento de Módulo e Coesão

A organização implementa funções de segurança como módulos amplamente independentes, que maximizam a coesão interna dos módulos e minimizam o acoplamento entre os módulos.  
Guia Adicional: A redução nas interações entre módulos ajuda a restringir as funções de segurança e a gerenciar a complexidade. Os conceitos de acoplamento e coesão são importantes no que diz respeito à modularidade no design de software. O acoplamento refere-se às dependências que um módulo possui de outros módulos. Coesão refere-se à relação entre as diferentes funções dentro de um módulo específico. Boas práticas de engenharia de software dependem de decomposição, camadas e minimização modulares para reduzir e gerenciar a complexidade, produzindo módulos de software altamente coesos e pouco acoplados.

### SC-3(5): Isolamento das Funções de Segurança | Estruturas em Camadas

A organização implementa funções de segurança como uma estrutura em camadas, minimizando as interações entre as camadas do design e evitando qualquer dependência das camadas inferiores da funcionalidade ou correção das camadas superiores.  
Guia Adicional: A implementação de estruturas em camadas com interações minimizadas entre funções de segurança e camadas sem loop (ou seja, funções da camada inferior não dependem de funções da camada superior) permite ainda mais o isolamento das funções de segurança e o gerenciamento da complexidade.

## SC-4: Informação em Recursos Compartilhados (P1)

**Descrição do Controle:**O sistema de informações evita a transferência não autorizada e não intencional de informações por meio de recursos compartilhados do sistema.  
  
**Guia Adicional:**Esse controle impede que as informações, incluindo representações criptografadas de informações, produzidas pelas ações de usuários / funções anteriores (ou pelas ações de processos que atuam em nome de usuários / funções anteriores) estejam disponíveis para quaisquer usuários / funções atuais (ou processos atuais) que obtenha acesso aos recursos compartilhados do sistema (por exemplo, registradores, memória principal, discos rígidos) após a liberação desses recursos nos sistemas de informação. O controle de informações em recursos compartilhados também é conhecido como reutilização de objetos e proteção de informações residuais. Este controle não trata: (i) remanência de informações que se refere à representação residual de dados que foram nominalmente apagados ou removidos; (ii) canais secretos (incluindo canais de armazenamento e/ou temporização) onde os recursos compartilhados são manipulados para violar as restrições do fluxo de informações; ou (iii) componentes dentro de sistemas de informação para os quais existem apenas usuários / funções únicos.  
  
**Melhorias do Controle:**

### SC-4(1): Informação em Recursos Compartilhados | Níveis de Segurança

[Retirado: Incorporado ao SC-4].

### SC-4(2): Informação em Recursos Compartilhados | Processamento de Períodos

O sistema de informações evita a transferência não autorizada de informações por meio de recursos compartilhados, de acordo com [Atribuição: procedimentos definidos pela organização] quando o processamento do sistema alterna explicitamente entre diferentes níveis de classificação de informações ou categorias de segurança.  
Guia Adicional: Esse aprimoramento de controle se aplica quando há alterações explícitas nos níveis de processamento de informações durante as operações do sistema de informações, por exemplo, durante o processamento multinível e o processamento de períodos com informações em diferentes níveis de classificação ou categorias de segurança. Os procedimentos definidos pela organização podem incluir, por exemplo, processos de higienização aprovados para informações armazenadas eletronicamente.

## SC-5: Proteção sobre Negação de Serviço (DoS) (P1)

**Descrição do Controle:**O sistema de informações protege contra ou limita os efeitos dos seguintes tipos de ataques de negação de serviço: [Atribuição: tipos de ataques de negação de serviço definidos pela organização ou referências a fontes dessas informações] empregando [Atribuição: salvaguardas de segurança definidas pela organização] .  
  
**Guia Adicional:**Existe uma variedade de tecnologias para limitar ou, em alguns casos, eliminar os efeitos dos ataques de negação de serviço. Por exemplo, os dispositivos de proteção de limite podem filtrar certos tipos de pacotes para proteger os componentes do sistema de informações nas redes organizacionais internas contra serem diretamente afetados por ataques de negação de serviço. O emprego de maior capacidade e largura de banda combinadas com redundância de serviço também pode reduzir a suscetibilidade a ataques de negação de serviço.  
  
**Melhorias do Controle:**

### SC-5(1): Proteção sobre Negação de Serviço (DoS) | Usuários Internos Restritos

O sistema de informação restringe a capacidade dos indivíduos de lançar [Atribuição: ataques de negação de serviço definidos pela organização] contra outros sistemas de informação.  
Guia Adicional: Restringir a capacidade de indivíduos de iniciar ataques de negação de serviço requer que os mecanismos usados para esses ataques estejam indisponíveis. Os indivíduos preocupados podem incluir, por exemplo, insiders hostis ou adversários externos que violaram com êxito o sistema de informações e estão usando o sistema como plataforma para lançar ataques cibernéticos a terceiros. As organizações podem restringir a capacidade dos indivíduos de conectar e transmitir informações arbitrárias no meio de transporte (ou seja, rede, espectro sem fio). As organizações também podem limitar a capacidade dos indivíduos de usar recursos excessivos do sistema de informações. A proteção contra indivíduos com a capacidade de iniciar ataques de negação de serviço pode ser implementada em sistemas de informações específicos ou em dispositivos de fronteira que proíbem a saída para potenciais sistemas de destino.

### SC-5(2): Proteção sobre Negação de Serviço (DoS) | Capacidade de Excesso / Largura de Banda / Redundância

O sistema de informações gerencia excesso de capacidade, largura de banda ou outra redundância para limitar os efeitos dos ataques de negação de serviço de inundação de informações.  
Guia Adicional: O gerenciamento do excesso de capacidade garante a disponibilidade de capacidade suficiente para combater ataques de inundação. O gerenciamento do excesso de capacidade pode incluir, por exemplo, o estabelecimento de prioridades de uso, cotas ou particionamento selecionados.

### SC-5(3): Proteção sobre Negação de Serviço (DoS) | Detecção / Monitoramento

A organização:  
  
a. Emprega [Atribuição: ferramentas de monitoramento definidas pela organização] para detectar indicadores de ataques de negação de serviço contra o sistema de informação; e  
  
b. Monitora [Atribuição: recursos do sistema de informações definidas pela organização] para determinar se existem recursos suficientes para impedir ataques efetivos de negação de serviço.  
Guia Adicional: As organizações consideram a utilização e a capacidade dos recursos do sistema de informações ao gerenciar os riscos de negação de serviço devido a ataques maliciosos. Os ataques de negação de serviço podem se originar de fontes externas ou internas. Os recursos do sistema de informações sensíveis à negação de serviço incluem, por exemplo, armazenamento físico em disco, memória e ciclos de CPU. As salvaguardas comuns para evitar ataques de negação de serviço relacionados à utilização e capacidade de armazenamento incluem, por exemplo, instituir cotas de disco, configurar sistemas de informações para alertar automaticamente os administradores quando limites específicos de capacidade de armazenamento forem atingidos, usar tecnologias de compactação de arquivos para maximizar o espaço de armazenamento disponível e impor partições separadas para dados do sistema e do usuário.

## SC-6: Disponibilidade de Recursos (P0)

**Descrição do Controle:**O sistema de informações protege a disponibilidade de recursos alocando [Atribuição: recursos definidos pela organização] por [Seleção (um ou mais); prioridade; contingente; [Atribuição: salvaguardas de segurança definidas pela organização]].  
  
**Guia Adicional:**A proteção de prioridade ajuda a impedir que os processos de prioridade mais baixa atrasem ou interfiram no sistema de informações que atende a quaisquer processos de prioridade mais alta. As cotas impedem que usuários ou processos obtenham mais do que quantidades predeterminadas de recursos. Este controle não se aplica aos componentes do sistema de informações para os quais existem apenas usuários / funções únicos.

## SC-7: Proteção de Borda (P1)

**Descrição do Controle:**O sistema de informação:  
  
a. Monitora e controla as comunicações nos limites externos do sistema e nos principais limites internos do sistema;  
  
b. Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamente; logicamente] separados das redes organizacionais internas; e  
  
c. Conecta-se a redes ou sistemas de informação externos apenas por meio de interfaces gerenciadas que consistem em dispositivos de proteção de limite organizados de acordo com uma arquitetura de segurança organizacional.  
  
**Guia Adicional:**As interfaces gerenciadas incluem, por exemplo, gateways, roteadores, firewalls, guardas, análise de código malicioso com base em rede e sistemas de virtualização ou túneis criptografados implementados em uma arquitetura de segurança (por exemplo, roteadores que protegem firewalls ou gateways de aplicativos que residem em sub-redes protegidas). As sub-redes separadas física ou logicamente das redes internas são chamadas de zonas desmilitarizadas ou DMZs. Restringir ou proibir interfaces em sistemas de informações organizacionais inclui, por exemplo, restringir o tráfego da Web externo a servidores da Web designados em interfaces gerenciadas e proibir o tráfego externo que parece estar falsificando endereços internos. As organizações consideram a natureza compartilhada dos serviços comerciais de telecomunicações na implementação de controles de segurança associados ao uso de tais serviços. Os serviços de telecomunicações comerciais são geralmente baseados em componentes de rede e sistemas de gerenciamento consolidado compartilhados por todos os clientes comerciais conectados e também podem incluir linhas de acesso fornecidas por terceiros e outros elementos de serviço. Esses serviços de transmissão podem representar fontes de maior risco, apesar das disposições de segurança do contrato.  
  
**Melhorias do Controle:**

### SC-7(1): Proteção de Borda | Subredes Fisicamente Separadas

[Retirado: Incorporado ao SC-7].

### SC-7(2): Proteção de Borda | Acesso Público

[Retirado: Incorporado ao SC-7].

### SC-7(3): Proteção de Borda | Pontos de Acesso

A organização limita o número de conexões de rede externas ao sistema de informações.  
Guia Adicional: Limitar o número de conexões de rede externas facilita o monitoramento mais abrangente do tráfego de comunicações de entrada e saída. A iniciativa Conexão Confiável à Internet (TIC) é um exemplo de limitação do número de conexões de rede externas.

### SC-7(4): Proteção de Borda | Serviços Externos de Telecomunicações

A organização:  
  
a. Implementa uma interface gerenciada para cada serviço de telecomunicações externo;  
  
b. Estabelece uma política de fluxo de tráfego para cada interface gerenciada;  
  
c. Protege a confidencialidade e a integridade das informações transmitidas em cada interface;  
  
d. Documenta cada exceção à política de fluxo de tráfego com uma necessidade de missão / negócios de suporte e a duração dessa necessidade; e  
  
e. Revisa as exceções à política de fluxo de tráfego [Atribuição: frequência definida pela organização] e remove as exceções que não são mais suportadas por uma missão explícita / necessidade comercial.

### SC-7(5): Proteção de Borda | Negar por Padrão / Permitir por Exceção

O sistema de informações nas interfaces gerenciadas nega o tráfego de comunicações da rede por padrão e permite o tráfego de comunicações da rede por exceção (ou seja, negar tudo, permitir por exceção).  
Guia Adicional: Esse aprimoramento de controle se aplica ao tráfego de comunicações de rede de entrada e saída. Uma política de tráfego de comunicações de rede de negar tudo, permitir por exceção, garante que apenas as conexões essenciais e aprovadas sejam permitidas.

### SC-7(6): Proteção de Borda | Resposta a Falhas Reconhecidas

[Retirado: Incorporado no SC-7 (18)].

### SC-7(7): Proteção de Borda | Impedir o Túnel Dividido para Dispositivos Remotos

O sistema de informações, em conjunto com um dispositivo remoto, impede que o dispositivo estabeleça simultaneamente conexões não remotas com o sistema e se comunique através de alguma outra conexão com recursos em redes externas.  
Guia Adicional: Esse aprimoramento de controle é implementado em dispositivos remotos (por exemplo, computadores notebook) por meio de definições de configuração para desativar o túnel dividido nesses dispositivos e impedindo que essas definições sejam prontamente configuráveis pelos usuários. Esse aprimoramento de controle é implementado no sistema de informações pela detecção de tunelamento dividido (ou de definições de configuração que permitem o tunelamento dividido) no dispositivo remoto e proibindo a conexão se o dispositivo remoto estiver usando o tunelamento dividido. O túnel dividido pode ser desejável por usuários remotos para se comunicar com recursos locais do sistema de informações, como impressoras / servidores de arquivos. No entanto, o túnel dividido permitiria conexões externas não autorizadas, tornando o sistema mais vulnerável a ataques e exfiltração de informações organizacionais. O uso de VPNs para conexões remotas, quando provisionado adequadamente com os controles de segurança apropriados, pode fornecer à organização garantia suficiente de que pode tratar efetivamente essas conexões como conexões não remotas da perspectiva de confidencialidade e integridade. As VPNs, portanto, fornecem um meio para permitir caminhos de comunicação não remotos a partir de dispositivos remotos. O uso de uma VPN provisionada adequadamente não elimina a necessidade de impedir o tunelamento dividido.

### SC-7(8): Proteção de Borda | Rota do Tráfego para Servidores Autenticados

O sistema de informações roteia [Atribuição: tráfego de comunicação interno definido pela organização] para [Atribuição: redes externas definidas pela organização] através de servidores proxy autenticados em interfaces gerenciadas.  
Guia Adicional: Redes externas são redes fora do controle organizacional. Um servidor proxy é um servidor (ou seja, sistema ou aplicativo de informações) que atua como intermediário para clientes que solicitam recursos do sistema de informações (por exemplo, arquivos, conexões, páginas da web ou serviços) de outros servidores organizacionais. As solicitações do cliente estabelecidas por meio de uma conexão inicial com o servidor proxy são avaliadas para gerenciar a complexidade e fornecer proteção adicional, limitando a conectividade direta. Os dispositivos de filtragem de conteúdo da Web são um dos servidores proxy mais comuns que fornecem acesso à Internet. Os servidores proxy suportam o registro de sessões individuais do Transmission Control Protocol (TCP) e o bloqueio de URLs (Uniform Resource Locators) específicos, nomes de domínio e endereços IP (Internet Protocol). Os proxies da Web podem ser configurados com listas definidas pela organização de sites autorizados e não autorizados.

### SC-7(9): Proteção de Borda | Tráfego Restritivo de Comunicações de Saída de Ameaça

O sistema de informação:  
  
a. Detecta e nega o tráfego de comunicações de saída que representa uma ameaça para sistemas de informações externos; e  
  
b. Audita a identidade dos usuários internos associados às comunicações negadas.  
Guia Adicional: A detecção do tráfego de comunicações de saída de ações internas que podem representar ameaças a sistemas de informações externos é às vezes denominada detecção de extrusão. A detecção de extrusão nos limites do sistema de informações como parte das interfaces gerenciadas inclui a análise do tráfego de comunicações recebidas e enviadas, buscando indicações de ameaças internas à segurança de sistemas externos. Essas ameaças incluem, por exemplo, tráfego indicativo de ataques de negação de serviço e tráfego contendo código malicioso.

### SC-7(10): Proteção de Borda | Impedir a Exfiltração Não Autorizada

A organização impede a exfiltração não autorizada de informações nas interfaces gerenciadas.  
Guia Adicional: As salvaguardas implementadas pelas organizações para impedir a exfiltração não autorizada de informações dos sistemas de informação incluem, por exemplo: (i) adesão estrita aos formatos de protocolo; (ii) monitoramento de sinalização de sistemas de informação; (iii) monitoramento de esteganografia; (iv) desconectar interfaces de rede externas, exceto quando explicitamente necessário; (v) desmontar e remontar cabeçalhos de pacotes; e (vi) empregar análise de perfil de tráfego para detectar desvios em relação ao volume / tipos de tráfego esperado nas organizações ou retornos de chamada para os centros de comando e controle. Os dispositivos que impõem aderência estrita aos formatos de protocolo incluem, por exemplo, firewalls de inspeção profunda de pacotes e gateways XML. Esses dispositivos verificam a aderência aos formatos e especificações de protocolo na camada de aplicativo e servem para identificar vulnerabilidades que não podem ser detectadas por dispositivos que operam na rede ou nas camadas de transporte. Esse aprimoramento de controle está intimamente associado a soluções entre domínios e guardas do sistema que impõem requisitos de fluxo de informações.

### SC-7(11): Proteção de Borda | Tráfego Restritivo de Comunicações

O sistema de informações permite apenas que as comunicações recebidas de [Atribuição: fontes autorizadas definidas pela organização] sejam roteadas para [Atribuição: destinos autorizados definidos pela organização].  
Guia Adicional: Esse aprimoramento de controle fornece determinações de que os pares de endereços de origem e destino representam comunicações autorizadas / permitidas. Essas determinações podem se basear em vários fatores, incluindo, por exemplo, a presença de pares de endereços de origem / destino em listas de comunicações autorizadas / permitidas, a ausência de pares de endereços em listas de pares não autorizados / não permitidos ou o cumprimento de regras mais gerais para / pares de origem / destino permitidos.

### SC-7(12): Proteção de Borda | Proteção Baseada em Host

A organização implementa [Atribuição: mecanismos de proteção de limite baseados em host definidos pela organização] em [Atribuição: componentes do sistema de informações definidos pela organização].  
Guia Adicional: Os mecanismos de proteção de limite baseados em host incluem, por exemplo, firewalls baseados em host. Os componentes do sistema de informações que empregam mecanismos de proteção de limites baseados em host incluem, por exemplo, servidores, estações de trabalho e dispositivos móveis.

### SC-7(13): Proteção de Borda | Isolamento de Ferramentas de Segurança / Mecanismos / Componentes de Suporte

A organização isola [Atribuição: ferramentas, mecanismos e componentes de suporte de segurança definidos pela organização] de outros componentes internos do sistema de informação implementando sub-redes fisicamente separadas com interfaces gerenciadas para outros componentes do sistema.  
Guia Adicional: Sub-redes fisicamente separadas com interfaces gerenciadas são úteis, por exemplo, no isolamento de defesas de redes de computadores de redes críticas de processamento operacional para impedir que adversários descubram a análise e as técnicas forenses das organizações.

### SC-7(14): Proteção de Borda | Proteção Contra Conexões Físicas Não Autorizadas

A organização protege contra conexões físicas não autorizadas em [Atribuição: interfaces gerenciadas definidas pela organização].  
Guia Adicional: Os sistemas de informação que operam em diferentes categorias de segurança ou níveis de classificação podem compartilhar controles físicos e ambientais comuns, uma vez que os sistemas podem compartilhar espaço dentro das instalações da organização. Na prática, é possível que esses sistemas de informação separados compartilhem salas de equipamentos comuns, armários de fiação e caminhos de distribuição de cabos. A proteção contra conexões físicas não autorizadas pode ser alcançada, por exemplo, empregando bandejas de cabos, quadros de conexão e painéis de conexões claramente identificados e fisicamente separados para cada lado das interfaces gerenciadas com controles de acesso físico que impõem acesso limitado a esses itens.

### SC-7(15): Proteção de Borda | Acessos de Rota Privilegiadas da Rede

O sistema de informações roteia todos os acessos privilegiados em rede por meio de uma interface gerenciada dedicada para fins de controle de acesso e auditoria.

### SC-7(16): Proteção de Borda | Evitar a Descoberta de Componentes/Dispositivos

O sistema de informações impede a descoberta de componentes específicos do sistema que compõem uma interface gerenciada.  
Guia Adicional: Esse aprimoramento de controle protege os endereços de rede dos componentes do sistema de informações que fazem parte das interfaces gerenciadas, desde a descoberta até as ferramentas e técnicas comuns usadas para identificar dispositivos nas redes. Os endereços de rede não estão disponíveis para descoberta (por exemplo, endereço de rede não publicado ou inserido nos sistemas de nomes de domínio), exigindo conhecimento prévio para acesso. Outra técnica de ofuscação é alterar periodicamente os endereços de rede.

### SC-7(17): Proteção de Borda | Aplicação Automatizada dos Formatos do Protocolo

O sistema de informações reforça a aderência aos formatos de protocolo.  
Guia Adicional: Os componentes do sistema de informações que aplicam os formatos de protocolo incluem, por exemplo, firewalls de inspeção profunda de pacotes e gateways XML. Esses componentes do sistema verificam a aderência aos formatos / especificações do protocolo (por exemplo, IEEE) na camada de aplicação e identificam vulnerabilidades significativas que não podem ser detectadas por dispositivos que operam na rede ou nas camadas de transporte.

### SC-7(18): Proteção de Borda | Falha Segura

O sistema de informações falha com segurança no caso de uma falha operacional de um dispositivo de proteção de limite.  
Guia Adicional: A proteção contra falhas é uma condição alcançada pelo emprego de mecanismos do sistema de informações para garantir que, no caso de falhas operacionais dos dispositivos de proteção de limite nas interfaces gerenciadas (por exemplo, roteadores, firewalls, guardas e gateways de aplicativos que residam nas sub-redes protegidas, comumente chamadas de zonas desmilitarizadas) , os sistemas de informações não entram em estados não seguros onde as propriedades de segurança pretendidas não são mais mantidas. Falhas nos dispositivos de proteção de limites não podem levar a informações externas aos dispositivos, nem podem permitir liberações de informações não autorizadas.

### SC-7(19): Proteção de Borda | Bloca a Comunicação de Recursos Não Organizacionalmente Configurados

O sistema de informações bloqueia o tráfego de comunicações de entrada e saída entre [Atribuição: clientes de comunicação definidos pela organização] que são configurados independentemente por usuários finais e provedores de serviços externos.  
Guia Adicional: Os clientes de comunicação configurados independentemente por usuários finais e provedores de serviços externos incluem, por exemplo, clientes de mensagens instantâneas. O bloqueio de tráfego não se aplica a clientes de comunicação configurados por organizações para executar funções autorizadas.

### SC-7(20): Proteção de Borda | Isolamento / Segregação Dinâmica

O sistema de informações fornece a capacidade de isolar / segregar dinamicamente [Atribuição: componentes do sistema de informações definidos pela organização] de outros componentes do sistema.  
Guia Adicional: A capacidade de isolar ou segregar dinamicamente determinados componentes internos dos sistemas de informações organizacionais é útil quando é necessário particionar ou separar certos componentes de origem duvidosa daqueles componentes que possuem maior confiabilidade. O isolamento de componentes reduz a superfície de ataque dos sistemas de informações organizacionais. O isolamento de componentes selecionados do sistema de informações também é um meio de limitar os danos causados por ataques cibernéticos bem-sucedidos quando esses ataques ocorrem.

### SC-7(21): Proteção de Borda | Isolamento de Componentes do Sistema de Informação

A organização emprega mecanismos de proteção de limites para separar [Atribuição: componentes de sistemas de informações definidos pela organização] que apoia [Atribuição: missões definidas pela organização e/ou funções de negócios].  
Guia Adicional: As organizações podem isolar os componentes do sistema de informações executando diferentes missões e/ou funções de negócios. Esse isolamento limita o fluxo de informações não autorizadas entre os componentes do sistema e também oferece a oportunidade de implantar maiores níveis de proteção para os componentes selecionados. A separação de componentes do sistema com mecanismos de proteção de limite fornece a capacidade de aumentar a proteção de componentes individuais e controlar mais efetivamente os fluxos de informações entre esses componentes. Esse tipo de proteção aprimorada limita o dano potencial de ataques e erros cibernéticos. O grau de separação fornecida varia de acordo com os mecanismos escolhidos. Os mecanismos de proteção de limite incluem, por exemplo, roteadores, gateways e firewalls que separam os componentes do sistema em redes ou sub-redes fisicamente separadas, dispositivos entre domínios que separam sub-redes, técnicas de virtualização e fluxos de informações criptografadas entre os componentes do sistema usando chaves de criptografia distintas.

### SC-7(22): Proteção de Borda | Subredes Separadas para Conexão a Diferentes Domínios de Segurança

O sistema de informações implementa endereços de rede separados (ou seja, sub-redes diferentes) para conectar-se a sistemas em diferentes domínios de segurança.  
Guia Adicional: A decomposição de sistemas de informação em sub-redes ajuda a fornecer o nível apropriado de proteção para conexões de rede a diferentes domínios de segurança que contêm informações com diferentes categorias ou níveis de classificação.

### SC-7(23): Proteção de Borda | Desativar o Feedback do Envio por Falha na Validação do Protocolo

O sistema de informações desabilita o feedback dos remetentes em caso de falha na validação do formato do protocolo.  
Guia Adicional: A desativação do feedback para os remetentes quando houver uma falha no formato de validação de protocolo impede que os adversários obtenham informações que, de outra forma, não estariam disponíveis.

**Referências:**

|  |  |
| --- | --- |
| Publicações de Normas Federais de Processamento de Informações N.199 | http://csrc.nist.gov/publications/PubsFIPS.html#199 |
| Publicação Especial NIST 800-41 | https://csrc.nist.gov/publications/search?keywords-lg=800-41 |
| Publicação Especial NIST 800-77 | https://csrc.nist.gov/publications/search?keywords-lg=800-77 |

## SC-8: Confidencialidade e Integridade da Transmissão (P1)

**Descrição do Controle:**O sistema de informação protege a [Seleção (uma ou mais): confidencialidade; integridade] da informação transmitida.  
  
**Guia Adicional:**Esse controle se aplica às redes internas e externas e a todos os tipos de componentes do sistema de informação dos quais as informações podem ser transmitidas (por exemplo, servidores, dispositivos móveis, notebooks, impressoras, copiadoras, scanners, fax). Os caminhos de comunicação fora da proteção física de um limite controlado são expostos à possibilidade de interceptação e modificação. A proteção da confidencialidade e/ou integridade das informações organizacionais pode ser realizada por meios físicos (por exemplo, empregando sistemas de distribuição protegidos) ou por meios lógicos (por exemplo, empregando técnicas de criptografia). As organizações que confiam em provedores comerciais que oferecem serviços de transmissão como serviços de mercadorias, e não como serviços totalmente dedicados (ou seja, serviços que podem ser altamente especializados para as necessidades individuais dos clientes), podem achar difícil obter as garantias necessárias com relação à implementação dos controles de segurança necessários para a transmissão confidencialidade / integridade. Em tais situações, as organizações determinam que tipos de serviços de confidencialidade / integridade estão disponíveis nos pacotes comerciais padrão de serviços de telecomunicações. Se for inviável ou impraticável obter os controles de segurança e garantias de efetividade do controle por meio de veículos apropriados, as organizações implementam controles de segurança compensatórios apropriados ou aceitam explicitamente o risco adicional.  
  
**Melhorias do Controle:**

### SC-8(1): Confidencialidade e Integridade da Transmissão | Proteção Física Criptográfica ou Alternativa

O sistema de informação implementa mecanismos criptográficos para [Seleção (um ou mais): impedir a divulgação não autorizada de informações; detectar alterações nas informações] durante a transmissão, a menos que seja protegido por [Atribuição: salvaguardas físicas alternativas definidas pela organização].  
Guia Adicional: As informações criptografadas para transmissão protegem as informações contra divulgação e modificação não autorizadas. Os mecanismos criptográficos implementados para proteger a integridade das informações incluem, por exemplo, funções hash criptográficas que têm aplicação comum em assinaturas digitais, somas de verificação e códigos de autenticação de mensagens. As salvaguardas alternativas de segurança física incluem, por exemplo, sistemas de distribuição protegidos.

### SC-8(2): Confidencialidade e Integridade da Transmissão | Manuseio Pré/Pós-Transmissão

O sistema de informação mantém a [Seleção (uma ou mais): confidencialidade; integridade] das informações durante a preparação para a transmissão e durante a recepção.  
Guia Adicional: As informações podem ser divulgadas ou modificadas de maneira não intencional ou maliciosa durante a preparação para a transmissão ou durante a recepção, incluindo, por exemplo, durante a agregação, nos pontos de transformação do protocolo e durante a embalagem / descompactação. Essas divulgações ou modificações não autorizadas comprometem a confidencialidade ou integridade das informações.

### SC-8(3): Confidencialidade e Integridade da Transmissão | Proteção Criptográfica para Mensagens Externas

O sistema de informações implementa mecanismos criptográficos para proteger as mensagens externas, a menos que seja protegido por [Atribuição: salvaguardas físicas alternativas definidas pela organização].  
Guia Adicional: Esse aprimoramento de controle trata da proteção contra divulgação não autorizada de informações. As mensagens externas incluem, por exemplo, cabeçalhos de mensagens / informações de roteamento. Esse aprimoramento de controle impede a exploração de mensagens externas e se aplica a redes ou links internos e externos que podem ser visíveis para indivíduos que não são usuários autorizados. Às vezes, as informações de cabeçalho / roteamento são transmitidas sem criptografia, porque as informações não são adequadamente identificadas pelas organizações como tendo um valor significativo ou porque a criptografia das informações pode resultar em menor desempenho da rede e/ou custos mais altos. Salvaguardas físicas alternativas incluem, por exemplo, sistemas de distribuição protegidos.

### SC-8(4): Confidencialidade e Integridade da Transmissão | Tornar Aleatório/Ocultar as Comunicações

O sistema de informações implementa mecanismos criptográficos para ocultar ou tornar aleatório os padrões de comunicação, a menos que seja protegido por [Atribuição: salvaguardas físicas alternativas definidas pela organização].  
Guia Adicional: Esse aprimoramento de controle trata da proteção contra divulgação não autorizada de informações. Os padrões de comunicação incluem, por exemplo, frequência, períodos, quantidade e previsibilidade. Alterações nos padrões de comunicação podem revelar informações com valor de inteligência, especialmente quando combinadas com outras informações disponíveis relacionadas a missões / funções de negócios suportadas por sistemas de informações organizacionais. Esse aprimoramento de controle evita a derivação de inteligência com base em padrões de comunicação e se aplica a redes ou links internos e externos que podem ser visíveis para indivíduos que não são usuários autorizados. Criptografar os links e transmitir em padrões contínuos, fixos / aleatórios impede a derivação de inteligência dos padrões de comunicação do sistema. Salvaguardas físicas alternativas incluem, por exemplo, sistemas de distribuição protegidos.

**Referências:**

|  |  |
| --- | --- |
| Publicações de Normas Federais de Processamento de Informações N.140-2 | http://csrc.nist.gov/publications/PubsFIPS.html#140-2 |
| Publicações de Normas Federais de Processamento de Informações N.197 | http://csrc.nist.gov/publications/PubsFIPS.html#197 |
| Publicação Especial NIST 800-52 | https://csrc.nist.gov/publications/search?keywords-lg=800-52 |
| Publicação Especial NIST 800-77 | https://csrc.nist.gov/publications/search?keywords-lg=800-77 |
| Publicação Especial NIST 800-81 | https://csrc.nist.gov/publications/search?keywords-lg=800-81 |
| Publicação Especial NIST 800-113 | https://csrc.nist.gov/publications/search?keywords-lg=800-113 |
| CNSS - Apólice 15 | https://www.cnss.gov/policies.html |
| CNSS - NSTISSI N.7003 | http://www.cnss.gov/Assets/pdf/nstissi\_7003.pdf |

## SC-9: Confidencialidade da Transmissão (P0)

**Descrição do Controle:**[Retirado: Incorporado ao SC-8].

## SC-10: Desconexão de Rede (P2)

**Descrição do Controle:**O sistema de informações encerra a conexão de rede associada a uma sessão de comunicações no final da sessão ou após [Atribuição: período definido pela organização] de inatividade.  
  
**Guia Adicional:**Este controle se aplica a redes internas e externas. O encerramento de conexões de rede associadas a sessões de comunicação inclui, por exemplo, desalocar pares de endereços / portas TCP / IP associados no nível do sistema operacional ou desalocar atribuições de rede no nível do aplicativo se várias sessões de aplicativos estiverem usando um único sistema operacional conexão de rede de vários níveis. Os períodos de inatividade podem ser estabelecidos pelas organizações e incluem, por exemplo, períodos por tipo de acesso à rede ou para acessos específicos à rede.

## SC-11: Caminho Confiável (P0)

**Descrição do Controle:**O sistema de informações estabelece um caminho de comunicação confiável entre o usuário e as seguintes funções de segurança do sistema: [Atribuição: funções de segurança definidas pela organização para incluir, no mínimo, autenticação e re-autenticação do sistema de informações].  
  
**Guia Adicional:**Caminhos confiáveis são mecanismos pelos quais os usuários (por meio de dispositivos de entrada) podem se comunicar diretamente com funções de segurança de sistemas de informação com a garantia necessária para suportar políticas de segurança da informação. Os mecanismos podem ser ativados apenas por usuários ou pelas funções de segurança dos sistemas de informações organizacionais. As respostas do usuário por caminhos confiáveis são protegidas contra modificações ou divulgação em aplicativos não confiáveis. As organizações empregam caminhos confiáveis para conexões de alta segurança entre funções de segurança de sistemas de informação e usuários (por exemplo, durante logins do sistema). A imposição de caminhos de comunicação confiáveis geralmente é fornecida por meio de uma implementação que atende ao conceito de monitor de referência.

## SC-12: Estabelecimento e Gerenciamento de Chaves Criptográficas (P1)

**Descrição do Controle:**A organização estabelece e gerencia chaves criptográficas para a criptografia requerida empregada no sistema de informações de acordo com [Atribuição: requisitos definidos pela organização para geração, distribuição, armazenamento, acesso e destruição de chaves].  
  
**Guia Adicional:**O gerenciamento e estabelecimento de chaves criptográficas podem ser executados usando procedimentos manuais ou mecanismos automatizados com suporte a procedimentos manuais. As organizações definem os principais requisitos de gerenciamento de acordo com as leis federais aplicáveis, ordens executivas, diretrizes, regulamentos, políticas, padrões e orientações, especificando opções, níveis e parâmetros apropriados. As organizações gerenciam armazenamentos confiáveis para garantir que apenas as âncoras de confiança aprovadas estejam nesses armazenamentos confiáveis. Isso inclui certificados com visibilidade externa aos sistemas de informações organizacionais e certificados relacionados às operações internas dos sistemas.  
  
**Melhorias do Controle:**

### SC-12(1): Estabelecimento e Gerenciamento de Chaves Criptográficas | Disponibilidade

A organização mantém a disponibilidade de informações no caso de perda de chaves criptográficas pelos usuários.  
Guia Adicional: A garantia de chaves de criptografia é uma prática comum para garantir a disponibilidade em caso de perda de chaves (por exemplo, devido a uma senha esquecida).

### SC-12(2): Estabelecimento e Gerenciamento de Chaves Criptográficas | Chaves Simétricas

A organização produz, controla e distribui chaves criptográficas simétricas usando [Seleção: compatível com NIST FIPS; Tecnologia e processos de gerenciamento de chaves aprovados pela NSA.

### SC-12(3): Estabelecimento e Gerenciamento de Chaves Criptográficas | Chaves Assimétricas

A organização produz, controla e distribui chaves criptográficas assimétricas usando [Seleção: tecnologia e processos de gerenciamento de chaves aprovados pela NSA; certificados PKI classe 3 aprovados ou material de chave pré-posicionado; certificados PKI classe 3 ou classe 4 aprovados e tokens de segurança de hardware que protegem a chave privada do usuário].

### SC-12(4): Estabelecimento e Gerenciamento de Chaves Criptográficas | Certificados PKI

[Retirado: Incorporado ao SC-12].

### SC-12(5): Estabelecimento e Gerenciamento de Chaves Criptográficas | Certificados PKI / Tokens de Hardware

[Retirado: Incorporado ao SC-12].

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-56 | https://csrc.nist.gov/publications/search?keywords-lg=800-56 |
| Publicação Especial NIST 800-57 | https://csrc.nist.gov/publications/search?keywords-lg=800-57 |

## SC-13: Proteção Criptográfica (P1)

**Descrição do Controle:**O sistema de informações implementa [Atribuição: usos criptográficos definidos pela organização e tipo de criptografia necessários para cada uso] de acordo com as leis federais aplicáveis, ordens executivas, diretivas, diretivas, políticas, regulamentos e normas.  
  
**Guia Adicional:**A criptografia pode ser empregada para oferecer suporte a uma variedade de soluções de segurança, incluindo, por exemplo, a proteção de Informações Classificadas e Não Classificadas Controladas, o fornecimento de assinaturas digitais e a aplicação da separação de informações quando indivíduos autorizados têm as liberações necessárias para essas informações, mas não possuem a garantia. Aprovações formais de acesso necessárias. A criptografia também pode ser usada para oferecer suporte à geração aleatória de números e geração de hash. Os padrões criptográficos geralmente aplicáveis incluem criptografia validada por FIPS e criptografia aprovada pela NSA. Esse controle não impõe nenhum requisito para as organizações usarem criptografia. No entanto, se a criptografia for necessária com base na seleção de outros controles de segurança, as organizações definem cada tipo de criptografia e o tipo de criptografia necessária (por exemplo, proteção de informações classificadas: criptografia aprovada pela NSA; fornecimento de assinaturas digitais: criptografia validada por FIPS) )  
  
**Melhorias do Controle:**

### SC-13(1): Proteção Criptográfica | Criptografia Validada por FIPS

[Retirado: Incorporado no SC-13].

### SC-13(2): Proteção Criptográfica | Criptografia Aprovada pela NSA

[Retirado: Incorporado no SC-13].

### SC-13(3): Proteção Criptográfica | Indivíduos sem Aprovações de Acesso Formal

[Retirado: Incorporado no SC-13].

### SC-13(4): Proteção Criptográfica | Assinaturas Digitais

[Retirado: Incorporado no SC-13].

**Referências:**

|  |  |
| --- | --- |
| Publicações de Normas Federais de Processamento de Informações N.140 | http://csrc.nist.gov/publications/PubsFIPS.html#140 |
| NIST - CSRC: Centro de Recursos de Segurança de Computadores | http://csrc.nist.gov/groups/STM/cmvp/index.html |
| CNSS: Comitê de Sistemas de Segurança Nacional | http://www.cnss.gov |

## SC-14: Proteções de Acesso Público (P0)

**Descrição do Controle:**[Retirado: capacidade fornecida por AC-2, AC-3, AC-5, AC-6, SI-3, SI-4, SI-5, SI-7, SI-10].

## SC-15: Dispositivos Colaborativos de Computação (P1)

**Descrição do Controle:**O sistema de informação:  
  
a. Proíbe a ativação remota de dispositivos de computação colaborativa com as seguintes exceções: [Atribuição: exceções definidas pela organização em que a ativação remota deve ser permitida]; e  
  
b. Fornece uma indicação explícita de uso para usuários fisicamente presentes nos dispositivos.  
  
**Guia Adicional:**Os dispositivos de computação colaborativa incluem, por exemplo, quadros brancos em rede, câmeras e microfones. A indicação explícita de uso inclui, por exemplo, sinais para os usuários quando dispositivos de computação colaborativos são ativados.  
  
**Melhorias do Controle:**

### SC-15(1): Dispositivos Colaborativos de Computação | Desconexão Física

O sistema de informações fornece uma desconexão física de dispositivos de computação colaborativa de uma maneira que ofereça facilidade de uso.  
Guia Adicional: Deixar de desconectar fisicamente os dispositivos de computação colaborativos pode resultar em comprometimentos subsequentes das informações da organização. O fornecimento de métodos fáceis para desconectar fisicamente esses dispositivos após uma sessão de computação colaborativa ajuda a garantir que os participantes efetuem a atividade de desconexão sem ter que passar por procedimentos complexos e tediosos.

### SC-15(2): Dispositivos Colaborativos de Computação | Tráfego de Comunicações Inbound/Outbound

[Retirado: Incorporado ao SC-7].

### SC-15(3): Dispositivos Colaborativos de Computação | Desativação/Remoção em Áreas de Trabalho Seguras

A organização desativa ou remove dispositivos de computação colaborativos de [Atribuição: sistemas de informação definidos pela organização ou componentes de sistema de informação] em [Atribuição: áreas de trabalho seguras definidas pela organização].  
Guia Adicional: Deixar de desativar ou remover dispositivos de computação colaborativos dos sistemas de informação ou componentes do sistema de informação pode resultar em comprometimentos subsequentes das informações da organização, incluindo, por exemplo, escutas nas conversas.

### SC-15(4): Dispositivos Colaborativos de Computação | Indicar Explicitamente Atuais Participantes

O sistema de informações fornece uma indicação explícita dos participantes atuais em [Tarefa: reuniões on-line definidas pela organização e teleconferências].  
Guia Adicional: Esse aprimoramento de controle ajuda a impedir que indivíduos não autorizados participem de sessões de computação colaborativa sem o conhecimento explícito de outros participantes.

## SC-16: Transmissão de Atributos de Segurança (P0)

**Descrição do Controle:**O sistema de informação associa [Atribuição: atributos de segurança definidos pela organização] às informações trocadas entre sistemas de informação e entre componentes do sistema.  
  
**Guia Adicional:**Os atributos de segurança podem ser explícita ou implicitamente associados às informações contidas nos sistemas de informações organizacionais ou nos componentes do sistema.

## SC-17: Certificados de Chave Pública da Infraestrutura (P1)

**Descrição do Controle:**A organização emite certificados de chave pública sob uma [atribuição: política de certificado definida pela organização] ou obtém certificados de chave pública de um provedor de serviços aprovado.  
  
**Guia Adicional:**Para todos os certificados, as organizações gerenciam armazenamentos confiáveis do sistema de informações para garantir que apenas âncoras confiáveis aprovadas estejam nos armazenamentos confiáveis. Esse controle aborda os certificados com visibilidade externa aos sistemas de informações organizacionais e os certificados relacionados às operações internas dos sistemas, por exemplo, serviços de horário específicos do aplicativo.

**Referências:**

|  |  |
| --- | --- |
| OMB Memorando 05-24 | https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2005/m05-24.pdf |
| Publicação Especial NIST 800-32 | https://csrc.nist.gov/publications/search?keywords-lg=800-32 |
| Publicação Especial NIST 800-63 | https://csrc.nist.gov/publications/search?keywords-lg=800-63 |

## SC-18: Código Móvel (P2)

**Descrição do Controle:**A organização:  
  
a. Define código móvel aceitável e inaceitável e tecnologias de código móvel;  
  
b. Estabelece restrições de uso e orientações de implementação para código móvel aceitável e tecnologias de código móvel; e  
  
c. Autoriza, monitora e controla o uso de código móvel no sistema de informações.  
  
**Guia Adicional:**As decisões relacionadas ao emprego de código móvel nos sistemas de informações organizacionais são baseadas no potencial do código de causar danos aos sistemas se usado com intuito malicioso. As tecnologias de código móvel incluem, por exemplo, Java, JavaScript, ActiveX, PostScript, PDF, filmes Shockwave, animações em Flash e VBScript. As restrições de uso e as diretrizes de implementação aplicam-se à seleção e uso de código móvel instalado em servidores e código móvel baixado e executado em estações de trabalho e dispositivos individuais (por exemplo, smartphones). A política e os procedimentos de código móvel abordam a prevenção do desenvolvimento, aquisição ou introdução de código móvel inaceitável nos sistemas de informações organizacionais.  
  
**Melhorias do Controle:**

### SC-18(1): Código Móvel | Identificar Código Inaceitável / Tomar Ações Corretivas

O sistema de informações identifica [Atribuição: código móvel inaceitável definido pela organização] e executa [Atribuição: ações corretivas definidas pela organização].  
Guia Adicional: As ações corretivas quando um código móvel inaceitável é detectado incluem, por exemplo, administradores de bloqueio, quarentena ou alerta. O bloqueio inclui, por exemplo, impedir a transmissão de arquivos de processamento de texto com macros incorporadas quando essas macros foram definidas como código móvel inaceitável.

### SC-18(2): Código Móvel | Aquisição / Desenvolvimento / Uso

A organização garante que a aquisição, desenvolvimento e uso do código móvel a ser implantado no sistema de informações atenda [Atribuição: requisitos de código móvel definidos pela organização].

### SC-18(3): Código Móvel | Evitar Download / Execução

O sistema de informações impede o download e a execução de [Atribuição: código móvel inaceitável definido pela organização

### SC-18(4): Código Móvel | Impedir a Execução Automática

O sistema de informações evita a execução automática do código móvel em [Atribuição: aplicativos de software definidos pela organização] e aplica [Atribuição: ações definidas pela organização] antes da execução do código.  
Guia Adicional: As ações aplicadas antes da execução do código móvel incluem, por exemplo, solicitar aos usuários antes de abrir anexos de correio eletrônico. Impedir a execução automática de código móvel inclui, por exemplo, desabilitar os recursos de execução automática nos componentes do sistema de informações que empregam dispositivos de armazenamento portáteis, como discos compactos (CDs), discos de vídeo digital (DVDs) e dispositivos USB (Universal Serial Bus).

### SC-18(5): Código Móvel | Permitir Execução apenas em Ambientes Confinados

A organização permite a execução de código apenas em ambientes virtuais confinados.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-28 | https://csrc.nist.gov/publications/search?keywords-lg=800-28 |
| Instruções do Departamento de Defesa dos EUA N.8551.01 | https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/855101p.pdf |

## SC-19: Protocolo de Voz por Internet (VOIP) (P1)

**Descrição do Controle:**A organização:  
  
a. Estabelece restrições de uso e diretrizes de implementação para tecnologias de Protocolo de Voz sobre Internet (VoIP), com base no potencial de causar danos ao sistema de informações, se usados maliciosamente; e  
  
b. Autoriza, monitora e controla o uso de VoIP no sistema de informação.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-58 | https://csrc.nist.gov/publications/search?keywords-lg=800-58 |

## SC-20: Serviço Seguro de Resolução de Nome/Endereço (Fonte Autoritária) (P1)

**Descrição do Controle:**O sistema de informação:  
  
a. Fornece autenticação adicional de origem de dados e artefatos de verificação de integridade, juntamente com os dados oficiais de resolução de nomes que o sistema retorna em resposta a consultas externas de resolução de nomes / endereços; e  
  
b. Fornece os meios para indicar o status de segurança das zonas filho e (se o filho oferecer suporte a serviços de resolução segura) para permitir a verificação de uma cadeia de confiança entre os domínios pai e filho, ao operar como parte de um espaço para nome hierárquico distribuído.  
  
**Guia Adicional:**Esse controle permite que clientes externos, incluindo, por exemplo, clientes remotos da Internet, obtenham garantias de autenticação de origem e verificação de integridade para o nome do host / serviço e informações de resolução de endereço de rede obtidas por meio do serviço. Os sistemas de informações que fornecem serviços de resolução de nomes e endereços incluem, por exemplo, servidores DNS (sistema de nomes de domínio). Artefatos adicionais incluem, por exemplo, assinaturas digitais de DNS Security (DNSSEC) e chaves criptográficas. Registros de recursos DNS são exemplos de dados autoritários. Os meios para indicar o status de segurança das zonas filho incluem, por exemplo, o uso de registros de recurso de assinante de delegação no DNS. Os controles de segurança DNS refletem (e são mencionados em) Memorando OMB 08-23. Os sistemas de informação que usam tecnologias diferentes do DNS para mapear entre nomes de host / serviço e endereços de rede fornecem outros meios para garantir a autenticidade e a integridade dos dados de resposta.  
  
**Melhorias do Controle:**

### SC-20(1): Serviço Seguro de Resolução de Nome/Endereço (Fonte Autoritária) | Subespaços Infantis

[Retirado: Incorporado no SC-20].

### SC-20(2): Serviço Seguro de Resolução de Nome/Endereço (Fonte Autoritária) | Origem / Integridade dos Dados

O sistema de informações fornece artefatos de proteção de integridade e origem de dados para consultas internas de resolução de nome / endereço.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-23 | https://csrc.nist.gov/publications/search?keywords-lg=800-23 |
| Publicação Especial NIST 800-81 | https://csrc.nist.gov/publications/search?keywords-lg=800-81 |

## SC-21: Serviço Seguro de Resolução de Nome/Endereço (Recursivo ou Caching) (P1)

**Descrição do Controle:**O sistema de informações solicita e executa autenticação de origem de dados e verificação de integridade dos dados nas respostas de resolução de nome / endereço que o sistema recebe de fontes autorizadas.  
  
**Guia Adicional:**Cada cliente dos serviços de resolução de nomes executa essa validação por conta própria ou possui canais autenticados para provedores de validação confiáveis. Os sistemas de informações que fornecem serviços de resolução de nomes e endereços para clientes locais incluem, por exemplo, servidores DNS (sistema de nomes de domínio) ou resolução recursiva. Os resolvedores de clientes DNS executam a validação de assinaturas DNSSEC ou os clientes usam canais autenticados para resolvedores recursivos que executam essas validações. Os sistemas de informação que usam tecnologias diferentes do DNS para mapear entre nomes de host / serviço e endereços de rede fornecem outros meios para permitir que os clientes verifiquem a autenticidade e a integridade dos dados de resposta.  
  
**Melhorias do Controle:**

### SC-21(1): Serviço Seguro de Resolução de Nome/Endereço (Recursivo ou Caching) | Origem / Integridade dos Dados

[Retirado: Incorporado no SC-21].

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-81 | https://csrc.nist.gov/publications/search?keywords-lg=800-81 |

## SC-22: Arquitetura e Provisão para Serviço de Resolução de Nome/Endereço (P1)

**Descrição do Controle:**Os sistemas de informações que coletivamente fornecem serviço de resolução de nome / endereço para uma organização são tolerantes a falhas e implementam a separação de função interna / externa.  
  
**Guia Adicional:**Os sistemas de informações que fornecem serviços de resolução de nomes e endereços incluem, por exemplo, servidores DNS (sistema de nomes de domínio). Para eliminar pontos únicos de falha e aprimorar a redundância, as organizações empregam pelo menos dois servidores de sistema de nomes de domínio com autoridade, um configurado como o servidor principal e o outro como o servidor secundário. Além disso, as organizações geralmente implantam os servidores em duas sub-redes de rede separadas geograficamente (ou seja, não localizadas na mesma instalação física). Para a separação de funções, os servidores DNS com funções internas processam apenas solicitações de resolução de nomes e endereços de dentro das organizações (ou seja, de clientes internos). Os servidores DNS com funções externas processam apenas solicitações de informações de resolução de nomes e endereços de clientes externos a organizações (ou seja, em redes externas, incluindo a Internet). As organizações especificam clientes que podem acessar servidores DNS autoritários em funções específicas (por exemplo, por intervalos de endereços, listas explícitas).

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-81 | https://csrc.nist.gov/publications/search?keywords-lg=800-81 |

## SC-23: Autenticidade da Sessão (P1)

**Descrição do Controle:**O sistema de informação protege a autenticidade das sessões de comunicação.  
  
**Guia Adicional:**Esse controle aborda a proteção de comunicações na sessão, em relação ao nível de pacote (por exemplo, sessões em arquiteturas orientadas a serviços que fornecem serviços baseados na Web) e estabelece motivos para confiança em ambas as extremidades das sessões de comunicação nas identidades contínuas de outras partes e na validade das informações transmitidas. A proteção de autenticidade inclui, por exemplo, proteção contra ataques do tipo intermediário / sequestro de sessão e inserção de informações falsas nas sessões.  
  
**Melhorias do Controle:**

### SC-23(1): Autenticidade da Sessão | Invalidar Identificadores de Sessões em Logout

O sistema de informações invalida os identificadores de sessão após o logout do usuário ou outro encerramento da sessão.  
Guia Adicional: Esse aprimoramento de controle reduz a capacidade dos adversários de capturar e continuar a empregar IDs de sessão válidos anteriormente.

### SC-23(2): Autenticidade da Sessão | Mensagem de Logouts Iniciados pelo Usuário

[Retirado: Incorporado ao AC-12 (1)].

### SC-23(3): Autenticidade da Sessão | Identificadores de Sessão Únicos Aleatórios

O sistema de informações gera um identificador de sessão exclusivo para cada sessão com [Atribuição: requisitos de aleatoriedade definidos pela organização] e reconhece apenas os identificadores de sessão gerados pelo sistema.  
Guia Adicional: Esse aprimoramento de controle reduz a capacidade dos adversários de reutilizar IDs de sessão válidos anteriormente. Empregar o conceito de aleatoriedade na geração de identificadores exclusivos de sessão ajuda a proteger contra ataques de força bruta para determinar futuros identificadores de sessão.

### SC-23(4): Autenticidade da Sessão | Identificadores de Sessão Únicos Aleatórios

[Retirado: Incorporado no SC-23 (3)].

### SC-23(5): Autenticidade da Sessão | Autoridades de Certificado Permitidas

O sistema de informações permite apenas o uso de [Atribuição: autoridades de certificação definidas pela organização] para verificar o estabelecimento de sessões protegidas.  
Guia Adicional: A dependência de autoridades de certificação (CAs) para o estabelecimento de sessões seguras inclui, por exemplo, o uso de certificados Secure Socket Layer (SSL) e/ou Transport Layer Security (TLS). Esses certificados, após verificação pelas respectivas autoridades de certificação, facilitam o estabelecimento de sessões protegidas entre clientes e servidores da Web.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-52 | https://csrc.nist.gov/publications/search?keywords-lg=800-52 |
| Publicação Especial NIST 800-77 | https://csrc.nist.gov/publications/search?keywords-lg=800-77 |
| Publicação Especial NIST 800-95 | https://csrc.nist.gov/publications/search?keywords-lg=800-95 |

## SC-24: Falha no Estado Conhecido (P1)

**Descrição do Controle:**O sistema de informações falha em um [Atribuição: estado conhecido definido pela organização] por [Atribuição: tipos de falhas definidos pela organização] preservando [Atribuição: informações de estado do sistema definido pela organização] em falha.  
  
**Guia Adicional:**A falha em um estado conhecido trata das preocupações de segurança de acordo com as necessidades de missão / negócios das organizações. A falha em um estado seguro conhecido ajuda a impedir a perda de confidencialidade, integridade ou disponibilidade de informações no caso de falhas nos sistemas de informações organizacionais ou nos componentes do sistema. A falha em um estado seguro conhecido ajuda a impedir que os sistemas falhem em um estado que pode causar ferimentos a pessoas ou destruir propriedades. A preservação das informações de estado do sistema de informações facilita a reinicialização do sistema e o retorno ao modo operacional das organizações, com menos interrupções nos processos de missão / negócios.

## SC-25: Thin Nodes (P0)

**Descrição do Controle:**A organização emprega [Atribuição: componentes do sistema de informações definidos pela organização] com funcionalidade e armazenamento de informações mínimos.  
  
**Guia Adicional:**A implantação de componentes do sistema de informação com funcionalidade reduzida / mínima (por exemplo, nós sem disco e tecnologias thin client) reduz a necessidade de proteger todos os pontos de extremidade do usuário e pode reduzir a exposição de informações, sistemas de informação e serviços a ataques cibernéticos.

## SC-26: Honeypots (P0)

**Descrição do Controle:**O sistema de informações inclui componentes projetados especificamente para serem alvo de ataques maliciosos com o objetivo de detectar, desviar e analisar esses ataques.  
  
**Guia Adicional:**Um honeypot é configurado como um engodo para atrair adversários e desviar seus ataques dos sistemas operacionais que suportam missões organizacionais / função comercial. Dependendo do uso específico do honeypot, pode ser necessário consultar o Escritório do Consultor Jurídico antes da implantação.  
  
**Melhorias do Controle:**

### SC-26(1): Honeypots | Detecção de Código Malicioso

[Retirado: Incorporado no SC-35].

## SC-27: Aplicações Independentes de Plataforma (P0)

**Descrição do Controle:**O sistema de informações inclui: [Atribuição: aplicativos independentes da plataforma definidos pela organização].  
  
**Guia Adicional:**Plataformas são combinações de hardware e software usadas para executar aplicativos de software. As plataformas incluem: (i) sistemas operacionais; (ii) as arquiteturas de computadores subjacentes, ou (iii) ambas. Aplicativos independentes de plataforma são aplicativos executados em várias plataformas. Tais aplicativos promovem portabilidade e reconstituição em diferentes plataformas, aumentando a disponibilidade de funções críticas nas organizações enquanto sistemas de informação com sistemas operacionais específicos estão sob ataque.

## SC-28: Proteção de Informação em Repouso (P1)

**Descrição do Controle:**O sistema de informação protege a [Seleção (uma ou mais): confidencialidade; integridade] de [Cessão: informações definidas pela organização em repouso].  
  
**Guia Adicional:**Esse controle aborda a confidencialidade e a integridade das informações em repouso e abrange as informações do usuário e do sistema. Informações em repouso se referem ao estado das informações quando localizadas nos dispositivos de armazenamento como componentes específicos dos sistemas de informação. As informações relacionadas ao sistema que exigem proteção incluem, por exemplo, configurações ou conjuntos de regras para firewalls, gateways, sistemas de detecção / prevenção de intrusões, roteadores de filtragem e conteúdo do autenticador. As organizações podem empregar mecanismos diferentes para obter proteções de confidencialidade e integridade, incluindo o uso de mecanismos criptográficos e a verificação de compartilhamento de arquivos. A proteção da integridade pode ser alcançada, por exemplo, com a implementação de tecnologias WORM (Write-Once-Read-Many). As organizações também podem empregar outros controles de segurança, incluindo, por exemplo, armazenamento off-line seguro no lugar do armazenamento on-line, quando não for possível obter uma proteção adequada das informações em repouso e/ou monitoramento contínuo para identificar códigos maliciosos em repouso.  
  
**Melhorias do Controle:**

### SC-28(1): Proteção de Informação em Repouso | Proteção Criptográfica

O sistema de informações implementa mecanismos criptográficos para impedir a divulgação e modificação não autorizadas de [Atribuição: informações definidas pela organização] em [Atribuição: componentes do sistema de informações definidas pela organização].  
Guia Adicional: A seleção de mecanismos criptográficos é baseada na necessidade de proteger a confidencialidade e a integridade das informações organizacionais. A força do mecanismo é proporcional à categoria de segurança e/ou classificação das informações. Esse aprimoramento de controle se aplica a concentrações significativas de mídia digital nas áreas organizacionais designadas para armazenamento de mídia e também a quantidades limitadas de mídia geralmente associadas aos componentes do sistema de informação em ambientes operacionais (por exemplo, dispositivos de armazenamento portáteis, dispositivos móveis). As organizações têm a flexibilidade de criptografar todas as informações em dispositivos de armazenamento (por exemplo, criptografia completa do disco) ou criptografar estruturas de dados específicas (por exemplo, arquivos, registros ou campos). As organizações que empregam mecanismos criptográficos para proteger as informações em repouso também consideram soluções de gerenciamento de chaves criptográficas.

### SC-28(2): Proteção de Informação em Repouso | Armazenagem Offline

A organização remove do armazenamento online e armazena off-line em um local seguro [Atribuição: informações definidas pela organização].  
Guia Adicional: A remoção de informações organizacionais do armazenamento do sistema de informações on-line para o armazenamento off-line elimina a possibilidade de os indivíduos obterem acesso não autorizado às informações por meio de uma rede. Portanto, as organizações podem optar por mover as informações para o armazenamento offline, em vez de proteger essas informações no armazenamento online.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-56 | https://csrc.nist.gov/publications/search?keywords-lg=800-56 |
| Publicação Especial NIST 800-57 | https://csrc.nist.gov/publications/search?keywords-lg=800-57 |
| Publicação Especial NIST 800-111 | https://csrc.nist.gov/publications/search?keywords-lg=800-111 |

## SC-29: Heterogeneidade (P0)

**Descrição do Controle:**A organização emprega um conjunto diversificado de tecnologias da informação para [Atribuição: componentes do sistema de informação definido pela organização] na implementação do sistema de informação.  
  
**Guia Adicional:**Aumentar a diversidade de tecnologias da informação nos sistemas de informações organizacionais reduz o impacto de possíveis explorações de tecnologias específicas e também se defende contra falhas de modo comum, incluindo aquelas induzidas por ataques da cadeia de suprimentos. A diversidade nas tecnologias da informação também reduz a probabilidade de os adversários usarem para comprometer um componente do sistema de informação ser igualmente eficaz em relação a outros componentes do sistema, aumentando ainda mais o fator de trabalho do adversário para concluir com êxito os ataques cibernéticos planejados. Um aumento na diversidade pode adicionar complexidade e sobrecarga de gerenciamento, o que pode levar a erros e configurações não autorizadas.  
  
**Melhorias do Controle:**

### SC-29(1): Heterogeneidade | Técnicas de Virtualização

A organização emprega técnicas de virtualização para dar suporte à implantação de uma diversidade de sistemas operacionais e aplicativos que são alterados [Atribuição: frequência definida pela organização].  
Guia Adicional: Embora mudanças frequentes nos sistemas operacionais e aplicativos apresentem desafios de gerenciamento de configuração, elas podem resultar em um fator de trabalho aumentado para os adversários, a fim de realizar ataques cibernéticos bem-sucedidos. A alteração de sistemas operacionais ou aplicativos virtuais, em oposição à alteração dos sistemas / aplicativos operacionais reais, fornece alterações virtuais que impedem o sucesso do invasor e reduzem os esforços de gerenciamento de configuração. Além disso, as técnicas de virtualização podem ajudar as organizações a isolar softwares não confiáveis e/ou softwares de procedência duvidosa em ambientes de execução confinados.

## SC-30: Ocultamento e Desorientação (P0)

**Descrição do Controle:**A organização emprega [Atribuição: técnicas de ocultação e má orientação definidas pela organização] para [Atribuição: sistemas de informações definidas pela organização] em [Atribuição: períodos de tempo definidos pela organização] para confundir e induzir em erro os adversários.  
  
**Guia Adicional:**As técnicas de ocultação e desvio de direção podem reduzir significativamente a capacidade de direcionamento dos adversários (isto é, janela de oportunidade e superfície de ataque disponível) para iniciar e concluir ataques cibernéticos. Por exemplo, as técnicas de virtualização fornecem às organizações a capacidade de disfarçar os sistemas de informações, reduzindo potencialmente a probabilidade de ataques bem-sucedidos sem o custo de ter várias plataformas. O aumento do uso de técnicas de ocultação / desvio de direção, incluindo, por exemplo, aleatoriedade, incerteza e virtualização, pode confundir e enganar suficientemente os adversários e, posteriormente, aumentar o risco de descoberta e/ou exposição da arte comercial. As técnicas de ocultação / desorientação também podem fornecer tempo adicional às organizações para desempenhar com êxito missões principais e funções de negócios. Devido ao tempo e esforço necessários para apoiar técnicas de ocultação / desvio de direção, prevê-se que essas técnicas sejam usadas pelas organizações em uma base muito limitada.  
  
**Melhorias do Controle:**

### SC-30(1): Ocultamento e Desorientação | Técnicas de Virtualização

[Retirado: Incorporado no SC-29 (1)].

### SC-30(2): Ocultamento e Desorientação | Aleatoriedade

A organização emprega [Atribuição: técnicas definidas pela organização] para introduzir a aleatoriedade nas operações e ativos organizacionais.  
Guia Adicional: A aleatoriedade introduz níveis crescentes de incerteza para os adversários em relação às ações que as organizações executam na defesa contra ataques cibernéticos. Tais ações podem impedir a capacidade dos adversários de direcionar corretamente os recursos de informações das organizações que apoiam missões críticas / funções de negócios. A incerteza também pode fazer com que os adversários hesitem antes de iniciar ou continuar ataques. As técnicas de direcionamento incorreto envolvendo aleatoriedade incluem, por exemplo, a execução de determinadas ações de rotina em diferentes horários do dia, o emprego de diferentes tecnologias da informação (por exemplo, navegadores, mecanismos de pesquisa), o uso de diferentes fornecedores e a alternância de papéis e responsabilidades do pessoal da organização.

### SC-30(3): Ocultamento e Desorientação | Alterar Locais de Processamento/Armazenamento

A organização altera o local de [Atribuição: processamento e/ou armazenamento definido pela organização] [Seleção: [Atribuição: frequência de tempo definida pela organização]; em intervalos aleatórios]].  
Guia Adicional: Os adversários visam missões organizacionais críticas / funções de negócios e os recursos de informação que apoiam essas missões e funções, ao mesmo tempo em que tentam minimizar a exposição de sua existência e de sua tradição. A natureza estática, homogênea e determinística dos sistemas de informações organizacionais direcionados pelos adversários torna esses sistemas mais suscetíveis a ataques cibernéticos, com menor custo e esforço do adversário para obter sucesso. A alteração dos locais de processamento e armazenamento organizacional (às vezes chamados de defesa de alvo em movimento) aborda a ameaça persistente avançada (APT) usando técnicas como virtualização, processamento distribuído e replicação. Isso permite que as organizações realoquem os recursos de informação (isto é, processamento e/ou armazenamento), dando suporte a missões críticas e funções de negócios. A alteração dos locais das atividades de processamento e/ou dos locais de armazenamento introduz incerteza nas atividades de direcionamento por parte dos adversários. Essa incerteza aumenta o fator de trabalho dos adversários, tornando os compromissos ou violações dos sistemas de informações organizacionais muito mais difíceis e demorados, e aumenta as chances de os adversários divulgarem inadvertidamente aspectos da arte comercial ao tentar localizar recursos organizacionais críticos.

### SC-30(4): Ocultamento e Desorientação | Informação Enganosa

A organização emprega informações realistas, mas enganosas, em [Atribuição: componentes do sistema de informações definidas pela organização] com relação ao seu estado ou postura de segurança.  
Guia Adicional: Esse aprimoramento de controle engana possíveis adversários em relação à natureza e extensão das salvaguardas de segurança implementadas pelas organizações. Como resultado, os adversários podem empregar técnicas de ataque incorretas (e, como resultado, ineficazes). Uma maneira de adversários enganosos é que as organizações coloquem informações enganosas sobre os controles de segurança específicos implantados em sistemas de informações externos que são conhecidos por serem acessados ou direcionados por adversários. Outra técnica é o uso de redes fraudulentas (por exemplo, redes de mel, ambientes virtualizados) que imitam aspectos reais dos sistemas de informações organizacionais, mas usam, por exemplo, configurações de software desatualizadas.

### SC-30(5): Ocultamento e Desorientação | Conceito de Componentes do Sistema

A organização emprega [Atribuição: técnicas definidas pela organização] para ocultar ou ocultar [Atribuição: componentes do sistema de informações definidas pela organização].  
Guia Adicional: Ao ocultar, disfarçar ou ocultar componentes críticos do sistema de informações, as organizações podem diminuir a probabilidade de os adversários atingirem e comprometerem com êxito esses ativos. Os meios possíveis para as organizações ocultar e/ou ocultar os componentes do sistema de informações incluem, por exemplo, a configuração de roteadores ou o uso de redes de mel ou técnicas de virtualização.

## SC-31: Análise de Canais de Cobertura (P0)

**Descrição do Controle:**A organização:  
  
a. Executa uma análise de canal secreto para identificar os aspectos das comunicações no sistema de informação que são avenidas potenciais para o encobrimento [Seleção (uma ou mais): armazenamento; canais]; e  
  
b. Estima a largura de banda máxima desses canais.  
  
**Guia Adicional:**Os desenvolvedores estão na melhor posição para identificar áreas em potencial dentro de sistemas que podem levar a canais secretos. A análise de canal encoberto é uma atividade significativa quando existe o potencial de fluxos de informações não autorizados entre domínios de segurança, por exemplo, no caso de sistemas de informações que contêm informações controladas por exportação e que têm conexões com redes externas (ou seja, redes não controladas por organizações). A análise de canal encoberto também é significativa para sistemas de informações multiníveis de segurança (MLS), sistemas de múltiplos níveis de segurança (MSL) e sistemas entre domínios.  
  
**Melhorias do Controle:**

### SC-31(1): Análise de Canais de Cobertura | Canais de Teste para Cobertura de Exploits

A organização testa um subconjunto dos canais secretos identificados para determinar quais canais são exploráveis.

### SC-31(2): Análise de Canais de Cobertura | Largura de Banda Máxima

A organização reduz a largura de banda máxima para a dissimulação identificada [Seleção (uma ou mais); armazenamento; tempo] canais para [Atribuição: valores definidos pela organização].  
Guia Adicional: Os desenvolvedores de sistemas de informações estão na melhor posição para reduzir a largura de banda máxima dos canais secretos e de armazenamento secretos identificados.

### SC-31(3): Análise de Canais de Cobertura | Medir a Largura de Banda em Ambientes Operacionais

A organização mede a largura de banda do [Atribuição: subconjunto definido pela organização dos canais secretos identificados] no ambiente operacional do sistema de informação.  
Guia Adicional: Esse aprimoramento de controle aborda a largura de banda de canal secreto em ambientes operacionais versus ambientes de desenvolvimento. Medir a largura de banda de canal secreto em ambientes operacionais ajuda as organizações a determinar quanta informação pode ser vazada secretamente antes que esse vazamento afete adversamente as missões organizacionais / funções de negócios. A largura de banda do canal secreto pode ser significativamente diferente quando medida nas configurações independentes dos ambientes específicos de operação (por exemplo, laboratórios ou ambientes de desenvolvimento).

## SC-32: Particionamento do Sistema de Informação (P0)

**Descrição do Controle:**A organização particiona o sistema de informações em [Atribuição: componentes do sistema de informações definidos pela organização] que residem em domínios ou ambientes físicos separados com base em [Atribuição: circunstâncias definidas pela organização para separação física de componentes].  
  
**Guia Adicional:**O particionamento do sistema de informações faz parte de uma estratégia de proteção de defesa em profundidade. As organizações determinam o grau de separação física dos componentes do sistema dos componentes fisicamente distintos em racks separados na mesma sala, para componentes em salas separadas para os componentes mais críticos, para uma separação geográfica mais significativa dos componentes mais críticos. A categorização de segurança pode orientar a seleção de candidatos apropriados para o particionamento de domínio. As interfaces gerenciadas restringem ou proíbem o acesso à rede e o fluxo de informações entre os componentes do sistema de informações particionados.

**Referências:**

|  |  |
| --- | --- |
| Publicações de Normas Federais de Processamento de Informações N.199 | http://csrc.nist.gov/publications/PubsFIPS.html#199 |

## SC-33: Integridade da Preparação da Transmissão (P0)

**Descrição do Controle:**[Retirado: Incorporado ao SC-8].

## SC-34: Programas Executáveis não Modificáveis (P0)

**Descrição do Controle:**O sistema de informação em [Atribuição: componentes do sistema de informações definidos pela organização]:  
  
a. Carrega e executa o ambiente operacional da mídia somente leitura aplicada por hardware; e  
  
b. Carrega e executa [Atribuição: aplicativos definidos pela organização] a partir de mídia somente leitura aplicada por hardware.  
  
**Guia Adicional:**O termo ambiente operacional é definido como o código específico que hospeda aplicativos, por exemplo, sistemas operacionais, executivos ou monitores, incluindo monitores de máquinas virtuais (ou seja, hypervisors). Também pode incluir certos aplicativos em execução diretamente nas plataformas de hardware. A mídia somente leitura aplicada por hardware inclui, por exemplo, unidades de disco graváveis em disco compacto (CD-R) / graváveis em disco de vídeo digital (DVD-R) e memória somente leitura programável única. O uso de armazenamento não modificável garante a integridade do software a partir do ponto de criação da imagem somente leitura. O uso de memória somente leitura reprogramável pode ser aceito como mídia somente leitura, desde que: (i) a integridade possa ser adequadamente protegida desde o ponto da gravação inicial até a inserção da memória no sistema de informação; e (ii) existem proteções de hardware confiáveis contra a reprogramação da memória enquanto instaladas nos sistemas de informações organizacionais.  
  
**Melhorias do Controle:**

### SC-34(1): Programas Executáveis não Modificáveis | Sem Armazenamento Escrita

A organização emprega [Atribuição: componentes do sistema de informações definidas pela organização] sem armazenamento gravável que seja persistente durante a reinicialização do componente ou a ativação / desativação.  
Guia Adicional: Esse aprimoramento de controle: (i) elimina a possibilidade de inserção de código malicioso por meio de armazenamento persistente e gravável nos componentes designados do sistema de informação; e (ii) se aplica ao armazenamento fixo e removível, com o último sendo tratado diretamente ou como restrições específicas impostas por meio de controles de acesso para dispositivos móveis.

### SC-34(2): Programas Executáveis não Modificáveis | Proteção da Integridade / Mídia Apenas Leitura

A organização protege a integridade das informações antes do armazenamento em mídia somente leitura e controla a mídia após a gravação dessas informações na mídia.  
Guia Adicional: As salvaguardas de segurança impedem a substituição de mídia em sistemas de informação ou a reprogramação de mídia somente leitura programável antes da instalação nos sistemas. As salvaguardas de segurança incluem, por exemplo, uma combinação de prevenção, detecção e resposta.

### SC-34(3): Programas Executáveis não Modificáveis | Proteção Baseada em Hardware

A organização:  
  
a. Emprega proteção contra gravação, baseada em hardware, para [Atribuição: componentes de firmware do sistema de informações definidos pela organização]; e  
  
b. Implementa procedimentos específicos para [Atribuição: indivíduos autorizados definidos pela organização] para desativar manualmente a proteção contra gravação de hardware para modificações de firmware e reativar a proteção contra gravação antes de retornar ao modo operacional.

## SC-35: Honeyclients (P0)

**Descrição do Controle:**O sistema de informações inclui componentes que procuram identificar de maneira proativa sites maliciosos e/ou código malicioso baseado na Web.  
  
**Guia Adicional:**Os clientes da Honey diferem dos honeypots, pois os componentes pesquisam ativamente a Internet em busca de códigos maliciosos (por exemplo, worms) contidos em sites externos. Assim como os honeypots, os clientes da honey exigem algumas medidas de isolamento de suporte (por exemplo, virtualização) para garantir que qualquer código malicioso descoberto durante a pesquisa e posteriormente executado não infecte os sistemas de informações organizacionais.

## SC-36: Processamento e Armazenamento Distribuído (P0)

**Descrição do Controle:**A organização distribui [Atribuição: processamento e armazenamento definidos pela organização] entre vários locais físicos.  
  
**Guia Adicional:**A distribuição de processamento e armazenamento em vários locais físicos fornece algum grau de redundância ou sobreposição para as organizações e, portanto, aumenta o fator de trabalho dos adversários para impactar negativamente as operações, ativos e indivíduos da organização. Esse controle não assume um único local de processamento ou armazenamento primário e, portanto, permite processamento e armazenamento paralelos.  
  
**Melhorias do Controle:**

### SC-36(1): Processamento e Armazenamento Distribuído | Técnicas de Votação

A organização emprega técnicas de pesquisa para identificar possíveis falhas, erros ou comprometimentos com [Atribuição: componentes de processamento e armazenamento distribuídos definidos pela organização].  
Guia Adicional: O processamento e/ou armazenamento distribuído podem ser empregados para reduzir as oportunidades de que os adversários comprometam com sucesso a confidencialidade, integridade ou disponibilidade de informações e sistemas de informação. No entanto, a distribuição de componentes de processamento e/ou armazenamento não impede que os adversários comprometam um (ou mais) dos componentes distribuídos. A pesquisa compara os resultados do processamento e/ou o conteúdo de armazenamento dos vários componentes distribuídos e, posteriormente, a votação dos resultados. A pesquisa identifica possíveis falhas, erros ou comprometimentos no processamento distribuído e/ou nos componentes de armazenamento.

## SC-37: Canais de Comunicação Fora do Padrão (Out-Of-Band) (P0)

**Descrição do Controle:**A organização emprega [Atribuição: canais fora de banda definidos pela organização] para entrega física ou transmissão eletrônica de [Atribuição: informações definidas pela organização, componentes do sistema de informações ou dispositivos] para [Atribuição: indivíduos ou sistemas de informação definidos pela organização ]  
  
**Guia Adicional:**Canais fora de banda incluem, por exemplo, acessos locais (não-rede) a sistemas de informação, caminhos de rede fisicamente separados dos caminhos de rede usados para tráfego operacional ou caminhos não-eletrônicos, como o Serviço Postal dos EUA. Isso contrasta com o uso dos mesmos canais (ou seja, canais em banda) que transportam tráfego operacional de rotina. Os canais fora da banda não têm a mesma vulnerabilidade / exposição que os canais dentro da banda e, portanto, os compromissos de confidencialidade, integridade ou disponibilidade dos canais dentro da banda não comprometem os canais fora da banda. As organizações podem empregar canais fora de banda na entrega ou transmissão de muitos itens organizacionais, incluindo, por exemplo, identificadores / autenticadores, alterações de gerenciamento de configuração de hardware, firmware ou software, informações de gerenciamento de chaves criptográficas, atualizações de segurança, backups de sistema / dados , informações de manutenção e atualizações de proteção de código malicioso.  
  
**Melhorias do Controle:**

### SC-37(1): Canais de Comunicação Fora do Padrão (Out-Of-Band) | Garantir Entrega/Transmissão

A organização emprega [Atribuição: salvaguardas de segurança definidas pela organização] para garantir que apenas [Atribuição: indivíduos ou sistemas de informações definidos pela organização] receba a [Atribuição: informações definidas pela organização, componentes do sistema de informações ou dispositivos].  
Guia Adicional: As técnicas e/ou métodos empregados pelas organizações para garantir que apenas sistemas ou indivíduos de informação designados recebam informações, componentes ou dispositivos de sistema específicos incluem, por exemplo, o envio de autenticadores por meio de serviço de courier, mas requerendo que os destinatários mostrem alguma forma de identificação fotográfica emitida pelo governo, como uma condição de recebimento.

## SC-38: Segurança das Operações (P0)

**Descrição do Controle:**A organização emprega [Atribuição: salvaguardas de segurança de operações definidas pela organização] para proteger as principais informações da organização durante todo o ciclo de vida de desenvolvimento do sistema.  
  
**Guia Adicional:**A segurança de operações (OPSEC) é um processo sistemático pelo qual os potenciais adversários podem receber informações negativas sobre os recursos e intenções das organizações, identificando, controlando e protegendo informações geralmente não classificadas que se relacionam especificamente ao planejamento e execução de atividades organizacionais sensíveis. O processo OPSEC envolve cinco etapas: (i) identificação de informações críticas (por exemplo, o processo de categorização de segurança); (ii) análise de ameaças; (iii) análise de vulnerabilidades; (iv) avaliação de riscos; e (v) a aplicação de contramedidas apropriadas. As proteções OPSEC são aplicadas aos sistemas de informações organizacionais e aos ambientes nos quais esses sistemas operam. As salvaguardas da OPSEC ajudam a proteger a confidencialidade das informações principais, incluindo, por exemplo, a limitação do compartilhamento de informações com fornecedores e potenciais fornecedores de componentes de sistemas de informação, produtos e serviços de tecnologia da informação e com outros elementos e indivíduos não organizacionais. As informações críticas para o sucesso da missão / negócios incluem, por exemplo, identidades de usuários, usos de elementos, fornecedores, processos da cadeia de suprimentos, requisitos funcionais e de segurança, especificações de design do sistema, protocolos de teste e detalhes de implementação de controle de segurança.

## SC-39: Isolamento do Processo (P1)

**Descrição do Controle:**O sistema de informações mantém um domínio de execução separado para cada processo de execução.  
  
**Guia Adicional:**Os sistemas de informação podem manter domínios de execução separados para cada processo de execução, atribuindo a cada processo um espaço de endereço separado. Cada processo do sistema de informações possui um espaço de endereço distinto, para que a comunicação entre os processos seja realizada de maneira controlada pelas funções de segurança, e um processo não pode modificar o código de execução de outro processo. A manutenção de domínios de execução separados para a execução de processos pode ser obtida, por exemplo, implementando espaços de endereço separados. Esse recurso está disponível na maioria dos sistemas operacionais comerciais que empregam tecnologias de processadores de vários estados.  
  
**Melhorias do Controle:**

### SC-39(1): Isolamento do Processo | Separação de Hardware

O sistema de informações implementa mecanismos subjacentes de separação de hardware para facilitar a separação de processos.  
Guia Adicional: A separação de processos do sistema de informações baseada em hardware é geralmente menos suscetível a comprometimentos do que a separação baseada em software, fornecendo maior garantia de que a separação será imposta. Os mecanismos subjacentes de separação de hardware incluem, por exemplo, gerenciamento de memória de hardware.

### SC-39(2): Isolamento do Processo | Isolamento Da Linha

O sistema de informações mantém um domínio de execução separado para cada thread em [Atribuição: processamento multithread definido pela organização].

## SC-40: Proteção de Link Sem Fio (P0)

**Descrição do Controle:**O sistema de informações protege [Atribuição: links sem fio definidos pela organização] de [Atribuição: tipos definidos pela organização de ataques de parâmetros de sinal ou referências a fontes para esses ataques].  
  
**Guia Adicional:**Esse controle se aplica a links de comunicação sem fio internos e externos que podem ser visíveis para indivíduos que não são usuários autorizados do sistema de informações. Os adversários podem explorar os parâmetros de sinal dos links sem fio se esses links não estiverem adequadamente protegidos. Existem muitas maneiras de explorar os parâmetros de sinal dos links sem fio para obter inteligência, negar serviço ou falsificar usuários de sistemas de informações organizacionais. Esse controle reduz o impacto de ataques exclusivos dos sistemas sem fio. Se as organizações dependem de provedores de serviços comerciais para serviços de transmissão como itens de commodities, e não como serviços totalmente dedicados, talvez não seja possível implementar esse controle.  
  
**Melhorias do Controle:**

### SC-40(1): Proteção de Link Sem Fio | Interferência Eletromagnética

O sistema de informação implementa mecanismos criptográficos que atingem [Atribuição: nível de proteção definido pela organização] contra os efeitos da interferência eletromagnética intencional.  
Guia Adicional: Esse aprimoramento de controle protege contra obstruções intencionais que podem negar ou prejudicar as comunicações, garantindo que as formas de onda do espectro de dispersão sem fio usadas para fornecer proteção anti-obstrução não sejam previsíveis por indivíduos não autorizados. O aprimoramento do controle também pode coincidentemente ajudar a mitigar os efeitos de interferência não intencional devido à interferência de transmissores legítimos que compartilham o mesmo espectro. Os requisitos da missão, as ameaças projetadas, o conceito de operações e a legislação, diretrizes, regulamentos, políticas, normas e diretrizes aplicáveis determinam os níveis de disponibilidade do link sem fio e o desempenho / criptografia necessário.

### SC-40(2): Proteção de Link Sem Fio | Reduza o Potencial de Detecção

O sistema de informação implementa mecanismos criptográficos para reduzir o potencial de detecção de links sem fio para [Atribuição: nível de redução definido pela organização].  
Guia Adicional: Esse aprimoramento de controle é necessário para comunicações secretas e para proteger transmissores sem fio de serem localizados geograficamente por suas transmissões. O aprimoramento do controle garante que as formas de onda do espectro de dispersão usadas para obter baixa probabilidade de detecção não sejam previsíveis por indivíduos não autorizados. Requisitos de missão, ameaças projetadas, conceito de operações e legislação, diretrizes, regulamentos, políticas, normas e diretrizes aplicáveis determinam os níveis nos quais os links sem fio devem ser indetectáveis.

### SC-40(3): Proteção de Link Sem Fio | Decepção de Comunicações Imitativas ou Manipulativas

O sistema de informação implementa mecanismos criptográficos para identificar e rejeitar as transmissões sem fio que são tentativas deliberadas de obter enganos imitativos ou manipulativos nas comunicações com base nos parâmetros do sinal.  
Guia Adicional: Esse aprimoramento de controle garante que os parâmetros de sinal das transmissões sem fio não sejam previsíveis por indivíduos não autorizados. Essa imprevisibilidade reduz a probabilidade de fraude imitativa ou manipulativa das comunicações com base apenas nos parâmetros do sinal.

### SC-40(4): Proteção de Link Sem Fio | Identificação dos Parâmetros de Sinal

O sistema de informação implementa mecanismos criptográficos para impedir a identificação de [Atribuição: transmissores sem fio definidos pela organização] usando os parâmetros de sinal do transmissor.  
Guia Adicional: As técnicas de impressão digital por rádio identificam os parâmetros de sinal exclusivos dos transmissores para a impressão digital desses transmissores para fins de rastreamento e identificação de missão / usuário. Esse aprimoramento de controle protege contra a identificação exclusiva de transmissores sem fio para fins de exploração de inteligência, garantindo que alterações anti-impressões digitais nos parâmetros do sinal não sejam previsíveis por indivíduos não autorizados. Esse aprimoramento de controle ajuda a garantir o sucesso da missão quando o anonimato é necessário.

## SC-41: Acesso a Porta e I/O do Dispositivo (P0)

**Descrição do Controle:**A organização desativa ou remove fisicamente [Atribuição: portas de conexão definidas pela organização ou dispositivos de entrada / saída] em [Atribuição: sistemas de informação definidos pela organização ou componentes do sistema de informação].  
  
**Guia Adicional:**As portas de conexão incluem, por exemplo, Universal Serial Bus (USB) e Firewire (IEEE 1394). Os dispositivos de entrada / saída (E / S) incluem, por exemplo, unidades Compact Disk (CD) e Digital Video Disk (DVD). Desativar ou remover fisicamente essas portas de conexão e dispositivos de E / S ajuda a impedir a exfiltração de informações dos sistemas de informação e a introdução de códigos maliciosos nos sistemas dessas portas / dispositivos.

## SC-42: Capacidade do Sensor e Dados (P0)

**Descrição do Controle:**O sistema de informação:  
  
a. Proíbe a ativação remota de recursos de detecção ambiental com as seguintes exceções: [Atribuição: exceções definidas pela organização em que a ativação remota de sensores é permitida]; e  
  
b. Fornece uma indicação explícita do uso do sensor para [Atribuição: classe de usuários definida pela organização].  
  
**Guia Adicional:**Esse controle geralmente se aplica a tipos de sistemas de informação ou componentes de sistema caracterizados como dispositivos móveis, por exemplo, smartphones, tablets e E-readers. Esses sistemas geralmente incluem sensores que podem coletar e registrar dados sobre o ambiente em que o sistema está em uso. Os sensores incorporados aos dispositivos móveis incluem, por exemplo, câmeras, microfones, mecanismos do sistema de posicionamento global (GPS) e acelerômetros. Embora os sensores nos dispositivos móveis ofereçam uma função importante, se ativados secretamente, esses dispositivos podem fornecer meios para que os adversários aprendam informações valiosas sobre indivíduos e organizações. Por exemplo, ativar remotamente a função GPS em um dispositivo móvel pode fornecer ao adversário a capacidade de rastrear os movimentos específicos de um indivíduo.  
  
**Melhorias do Controle:**

### SC-42(1): Capacidade do Sensor e Dados | Relatório a Indivíduos ou Papéis Autorizados

A organização garante que o sistema de informações esteja configurado para que os dados ou informações coletadas pelos [Atribuição: sensores definidos pela organização] sejam relatados apenas a indivíduos ou funções autorizados.  
Guia Adicional: Em situações em que os sensores são ativados por indivíduos autorizados (por exemplo, usuários finais), ainda é possível que os dados / informações coletados pelos sensores sejam enviados a entidades não autorizadas.

### SC-42(2): Capacidade do Sensor e Dados | Uso Autorizado

A organização emprega as seguintes medidas: [Atribuição: medidas definidas pela organização], para que os dados ou informações coletadas por [Atribuição: sensores definidos pela organização] sejam utilizados apenas para fins autorizados.  
Guia Adicional: As informações coletadas pelos sensores para uma finalidade específica autorizada potencialmente podem ser utilizadas indevidamente para alguma finalidade não autorizada. Por exemplo, os sensores de GPS usados para oferecer suporte à navegação no trânsito podem ser mal utilizados para rastrear movimentos de indivíduos. As medidas para mitigar essas atividades incluem, por exemplo, treinamento adicional para garantir que as partes autorizadas não abusem de sua autoridade ou (no caso em que os dados / informações do sensor sejam mantidos por terceiros) restrições contratuais ao uso dos dados / informações.

### SC-42(3): Capacidade do Sensor e Dados | Proibir o Uso de Dispositivos

A organização proíbe o uso de dispositivos que possuam [Atribuição: recursos de detecção ambiental definidos pela organização] em [Atribuição: instalações, áreas ou sistemas definidos pela organização].  
Guia Adicional: Por exemplo, as organizações podem proibir indivíduos de levar telefones celulares ou câmeras digitais para determinadas instalações ou áreas controladas específicas dentro de instalações onde informações classificadas são armazenadas ou conversas confidenciais estão ocorrendo.

## SC-43: Restrições de Uso (P0)

**Descrição do Controle:**A organização:  
  
a. Estabelece restrições de uso e diretrizes de implementação para [Atribuição: componentes do sistema de informações definidos pela organização] com base no potencial de causar danos ao sistema de informações, se usados maliciosamente; e  
  
b. Autoriza, monitora e controla o uso de tais componentes no sistema de informações.  
  
**Guia Adicional:**Os componentes do sistema de informações incluem componentes de hardware, software ou firmware (por exemplo, Protocolo de Voz sobre Internet, código móvel, copiadoras digitais, impressoras, scanners, dispositivos ópticos, tecnologias sem fio, dispositivos móveis).

## SC-44: Ambiente de Quarentena (P0)

**Descrição do Controle:**A organização emprega uma capacidade de câmara de detonação em [Tarefa: sistema de informações definido pela organização, componente do sistema ou local].  
  
**Guia Adicional:**As câmaras de detonação, também conhecidas como ambientes de execução dinâmica, permitem que as organizações abram anexos de e-mail, executam aplicativos não confiáveis ou suspeitos e executam solicitações de URL (Universal Resource Locator) na segurança de um ambiente isolado ou sandbox virtualizado. Esses ambientes de execução protegidos e isolados fornecem um meio de determinar se os anexos / aplicativos associados contêm código malicioso. Embora relacionado ao conceito de redes fraudulentas, o controle não se destina a manter um ambiente de longo prazo no qual os adversários possam operar e suas ações possam ser observadas. Em vez disso, pretende-se identificar rapidamente o código malicioso e reduzir a probabilidade de o código ser propagado para os ambientes de operação do usuário (ou impedir completamente essa propagação).

# SI - Integridade de Sistemas e Informação

## SI-1: Política e Procedimentos de Integridade do Sistema e da Informação (P1)

**Descrição do Controle:**A organização:  
  
a. Desenvolve, documenta e divulga para [Atribuição: pessoal ou funções definidas pela organização]:  
  
1. Uma política de integridade do sistema e das informações que atenda a finalidade, escopo, funções, responsabilidades, compromisso gerencial, coordenação entre entidades organizacionais e conformidade; e  
  
2. Procedimentos para facilitar a implementação da política de sistema e de integridade da informação e controles associados de sistema e integridade da informação; e  
  
b. Revisa e atualiza a atual:  
  
1. Política de integridade do sistema e das informações [Atribuição: frequência definida pela organização]; e  
  
2. Procedimentos de integridade do sistema e das informações [Tarefa: frequência definida pela organização].  
  
**Guia Adicional:**Esse controle aborda o estabelecimento de políticas e procedimentos para a implementação efetiva de controles de segurança selecionados e aprimoramentos de controle na família SI. As políticas e procedimentos refletem as leis federais aplicáveis, ordens executivas, diretivas, regulamentos, políticas, normas e diretrizes. Políticas e procedimentos do programa de segurança no nível da organização podem tornar desnecessária a necessidade de políticas e procedimentos específicos do sistema. A política pode ser incluída como parte da política geral de segurança da informação para organizações ou, inversamente, pode ser representada por múltiplas políticas refletindo a natureza complexa de certas organizações. Os procedimentos podem ser estabelecidos para o programa de segurança em geral e para sistemas de informação específicos, se necessário. A estratégia de gerenciamento de risco organizacional é um fator chave no estabelecimento de políticas e procedimentos.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-12 | https://csrc.nist.gov/publications/search?keywords-lg=800-12 |
| Publicação Especial NIST 800-100 | https://csrc.nist.gov/publications/search?keywords-lg=800-100 |

## SI-2: Remediação de Falhas (P1)

**Descrição do Controle:**A organização:  
  
a. Identifica, relata e corrige falhas do sistema de informações;  
  
b. Testa atualizações de software e firmware relacionadas à correção de falhas quanto à eficácia e possíveis efeitos colaterais antes da instalação;  
  
c. Instala atualizações de software e firmware relevantes para a segurança dentro de [Atribuição: período definido pela organização] do lançamento das atualizações; e  
  
d. Incorpora a correção de falhas no processo de gerenciamento da configuração organizacional.  
  
**Guia Adicional:**As organizações identificam sistemas de informações afetados por falhas de software anunciadas, incluindo possíveis vulnerabilidades resultantes dessas falhas, e relatam essas informações ao pessoal organizacional designado com responsabilidades de segurança da informação. As atualizações de software relevantes para a segurança incluem, por exemplo, patches, service packs, hot fixes e assinaturas de antivírus. As organizações também tratam de falhas descobertas durante avaliações de segurança, monitoramento contínuo, atividades de resposta a incidentes e tratamento de erros do sistema. As organizações aproveitam os recursos disponíveis, como os bancos de dados Common Weakness Enumeration (CWE) ou Common Vulnerabilities and Exposures (CVE), na correção de falhas descobertas em sistemas de informações organizacionais. Ao incorporar a correção de falhas nos processos de gerenciamento de configuração em andamento, as ações de correção necessárias / antecipadas podem ser rastreadas e verificadas. As ações de correção de falhas que podem ser rastreadas e verificadas incluem, por exemplo, determinar se as organizações seguem as orientações US-CERT e os alertas de vulnerabilidade de garantia de informações. Os períodos definidos pela organização para a atualização de software e firmware relevantes para a segurança podem variar com base em vários fatores, incluindo, por exemplo, a categoria de segurança do sistema de informações ou a criticidade da atualização (ou seja, gravidade da vulnerabilidade relacionada à descoberta) falha). Alguns tipos de correção de falhas podem exigir mais testes do que outros tipos. As organizações determinam o grau e o tipo de teste necessário para o tipo específico de atividade de correção de falhas em consideração e também os tipos de alterações que devem ser gerenciadas pela configuração. Em algumas situações, as organizações podem determinar que o teste de atualizações de software e/ou firmware não é necessário ou prático, por exemplo, ao implementar atualizações simples de assinatura de antivírus. As organizações também podem considerar nas decisões de teste se atualizações de software ou firmware relevantes à segurança são obtidas de fontes autorizadas com assinaturas digitais apropriadas.  
  
**Melhorias do Controle:**

### SI-2(1): Remediação de Falhas | Gestão Central

A organização gerencia centralmente o processo de correção de falhas.  
Guia Adicional: Gerenciamento central é o gerenciamento e a implementação em toda a organização de processos de correção de falhas. O gerenciamento central inclui o planejamento, a implementação, a avaliação, a autorização e o monitoramento dos controles de segurança de correção de falhas, gerenciados centralmente, definidos pela organização.

### SI-2(2): Remediação de Falhas | Estado Automatizado de Remediação de Falhas

A organização emprega mecanismos automatizados [Atribuição: frequência definida pela organização] para determinar o estado dos componentes do sistema de informações com relação à correção de falhas.

### SI-2(3): Remediação de Falhas | Tempo para Remediar Falhas / Marcas de Referência para Ações Corretivas

A organização:  
  
a. Mede o tempo entre a identificação e a correção de falhas; e  
  
b. Estabelece [Atribuição: benchmarks definidos pela organização] para a tomada de ações corretivas.  
Guia Adicional: Esse aprimoramento de controle exige que as organizações determinem o tempo atual necessário, em média, para corrigir falhas do sistema de informações após a identificação dessas falhas e, posteriormente, estabeleçam benchmarks organizacionais (ou seja, prazos) para a tomada de ações corretivas. Os benchmarks podem ser estabelecidos por tipo de falha e/ou gravidade da possível vulnerabilidade, se a falha puder ser explorada.

### SI-2(4): Remediação de Falhas | Ferramentas Automatizadas de Gerenciamento de Patches

[Retirado: Incorporado no SI-2].

### SI-2(5): Remediação de Falhas | Atualizações Automáticas de Software/Firmware

A organização instala [Atribuição: atualizações de firmware e software relevantes para a segurança definidas pela organização] automaticamente em [Atribuição: componentes do sistema de informações definidas pela organização].  
Guia Adicional: Devido a questões de integridade e disponibilidade do sistema de informações, as organizações consideram cuidadosamente a metodologia usada para realizar atualizações automáticas. As organizações devem equilibrar a necessidade de garantir que as atualizações sejam instaladas o mais rápido possível com a necessidade de manter o gerenciamento da configuração e com qualquer missão ou impacto operacional que as atualizações automáticas possam impor.

### SI-2(6): Remediação de Falhas | Remoção de Versões Anteriores de Software/Firmware

A organização remove [Atribuição: componentes de software e firmware definidos pela organização] após a instalação de versões atualizadas.  
Guia Adicional: Versões anteriores de componentes de software e/ou firmware que não são removidos do sistema de informações após a instalação das atualizações podem ser exploradas por adversários. Alguns produtos de tecnologia da informação podem remover automaticamente versões mais antigas de software e/ou firmware do sistema de informações.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-40 | https://csrc.nist.gov/publications/search?keywords-lg=800-40 |
| Publicação Especial NIST 800-128 | https://csrc.nist.gov/publications/search?keywords-lg=800-128 |

## SI-3: Proteção contra Código Malicioso (P1)

**Descrição do Controle:**A organização:  
  
a. Emprega mecanismos de proteção de código malicioso nos pontos de entrada e saída do sistema de informações para detectar e erradicar o código malicioso;  
  
b. Atualiza os mecanismos de proteção de código malicioso sempre que novas versões estão disponíveis, de acordo com a política e os procedimentos de gerenciamento de configuração organizacional;  
  
c. Configura mecanismos de proteção de código mal-intencionado para:  
  
1. Executar verificações periódicas do sistema de informações [Atribuição: frequência definida pela organização] e verificações em tempo real de arquivos de fontes externas em [Seleção (uma ou mais); ponto final; pontos de entrada / saída de rede] conforme os arquivos são baixados, abertos ou executados de acordo com a política de segurança organizacional; e  
  
2. [Seleção (um ou mais): bloqueia código malicioso; código malicioso em quarentena; envie alerta ao administrador; [Atribuição: ação definida pela organização]] em resposta à detecção de código malicioso; e  
  
d. Aborda o recebimento de falsos positivos durante a detecção e erradicação de códigos mal-intencionados e o impacto potencial resultante na disponibilidade do sistema de informações.  
  
**Guia Adicional:**Os pontos de entrada e saída do sistema de informação incluem, por exemplo, firewalls, servidores de correio eletrônico, servidores Web, servidores proxy, servidores de acesso remoto, estações de trabalho, notebooks e dispositivos móveis. O código malicioso inclui, por exemplo, vírus, worms, cavalos de Tróia e spyware. O código malicioso também pode ser codificado em vários formatos (por exemplo, UUENCODE, Unicode), contidos em arquivos compactados ou ocultos ou ocultos em arquivos usando esteganografia. O código malicioso pode ser transportado por diferentes meios, incluindo, por exemplo, acessos à Web, correio eletrônico, anexos de correio eletrônico e dispositivos de armazenamento portáteis. Inserções de código maliciosas ocorrem através da exploração de vulnerabilidades do sistema de informações. Os mecanismos de proteção de código malicioso incluem, por exemplo, definições de assinatura de antivírus e tecnologias baseadas em reputação. Existe uma variedade de tecnologias e métodos para limitar ou eliminar os efeitos do código malicioso. O gerenciamento invasivo da configuração e os controles abrangentes da integridade do software podem ser eficazes para impedir a execução de código não autorizado. Além do software comercial pronto para uso, o código malicioso também pode estar presente em softwares personalizados. Isso pode incluir, por exemplo, bombas lógicas, portas traseiras e outros tipos de ataques cibernéticos que podem afetar missões organizacionais / funções de negócios. Os mecanismos tradicionais de proteção de código malicioso nem sempre podem detectar esse código. Nessas situações, as organizações confiam em outras salvaguardas, incluindo, por exemplo, práticas seguras de codificação, gerenciamento e controle de configuração, processos confiáveis de compras e práticas de monitoramento para ajudar a garantir que o software não execute outras funções além das pretendidas. As organizações podem determinar que, em resposta à detecção de código malicioso, ações diferentes possam ser justificadas. Por exemplo, as organizações podem definir ações em resposta à detecção de código mal-intencionado durante verificações periódicas, ações em resposta à detecção de downloads maliciosos e/ou ações em resposta à detecção de mal-intencionados ao tentar abrir ou executar arquivos.  
  
**Melhorias do Controle:**

### SI-3(1): Proteção contra Código Malicioso | Gestão Central

A organização gerencia centralmente os mecanismos maliciosos de proteção de código.  
Guia Adicional: Gerenciamento central é o gerenciamento e a implementação em toda a organização de mecanismos de proteção de código malicioso. O gerenciamento central inclui o planejamento, a implementação, a avaliação, a autorização e o monitoramento dos controles de segurança de proteção contra códigos maliciosos, definidos pela organização e gerenciados centralmente.

### SI-3(2): Proteção contra Código Malicioso | Atualizações Automáticas

O sistema de informações atualiza automaticamente os mecanismos de proteção de código malicioso.  
Guia Adicional: Mecanismos de proteção de código malicioso incluem, por exemplo, definições de assinatura. Devido a questões de integridade e disponibilidade do sistema de informações, as organizações consideram cuidadosamente a metodologia usada para realizar atualizações automáticas.

### SI-3(3): Proteção contra Código Malicioso | Usuários Não Privilegiados

[Retirado: Incorporado ao AC-6 (10)].

### SI-3(4): Proteção contra Código Malicioso | Atualizações Somente por Usuários Privilegiados

O sistema de informações atualiza mecanismos de proteção de código mal-intencionado somente quando direcionado por um usuário privilegiado.  
Guia Adicional: Esse aprimoramento de controle pode ser apropriado para situações em que, por razões de segurança ou continuidade operacional, as atualizações são aplicadas apenas quando selecionadas / aprovadas pelo pessoal da organização designado.

### SI-3(5): Proteção contra Código Malicioso | Dispositivos Portáteis de Armazenamento

[Retirado: Incorporado ao MP-7].

### SI-3(6): Proteção contra Código Malicioso | Ensaio/Verificação

A organização:  
  
a. Testa mecanismos de proteção de código mal-intencionado [Atribuição: frequência definida pela organização], introduzindo um caso de teste benigno e não disseminado conhecido no sistema de informações; e  
  
b. Verifica se a detecção do caso de teste e os relatórios de incidentes associados ocorrem.

### SI-3(7): Proteção contra Código Malicioso | Detecção Baseada em Não Assinatura

O sistema de informações implementa mecanismos de detecção de código malicioso não baseados em assinaturas.  
Guia Adicional: Mecanismos de detecção não baseados em assinaturas incluem, por exemplo, o uso de heurísticas para detectar, analisar e descrever as características ou o comportamento de códigos maliciosos e fornecer salvaguardas contra códigos maliciosos para os quais ainda não existem assinaturas ou para quais assinaturas existentes ainda não existem. Isso inclui código malicioso polimórfico (ou seja, código que altera as assinaturas quando é replicado). Esse aprimoramento de controle não exclui o uso de mecanismos de detecção baseados em assinatura.

### SI-3(8): Proteção contra Código Malicioso | Detectar Comandos Não Autorizados

O sistema de informações detecta [Atribuição: comandos do sistema operacional não autorizado definidos pela organização] através da interface de programação de aplicativos do kernel em [Atribuição: componentes de hardware do sistema de informações definido pela organização] e [Seleção (um ou mais): emite um aviso; audita a execução do comando; impede a execução do comando].  
Guia Adicional: Esse aprimoramento de controle também pode ser aplicado a interfaces críticas que não sejam baseadas em kernel, incluindo, por exemplo, interfaces com máquinas virtuais e aplicativos privilegiados. Os comandos não autorizados do sistema operacional incluem, por exemplo, comandos para funções do kernel a partir de processos do sistema de informações que não são confiáveis para iniciar tais comandos ou comandos para funções do kernel suspeitas, embora os comandos desse tipo sejam razoáveis para o início dos processos. As organizações podem definir os comandos maliciosos a serem detectados por uma combinação de tipos de comando, classes de comando ou instâncias específicas de comandos. As organizações podem definir componentes de hardware por componente específico, tipo de componente, localização na rede ou combinação nela. As organizações podem selecionar ações diferentes para diferentes tipos / classes / instâncias específicas de comandos potencialmente maliciosos.

### SI-3(9): Proteção contra Código Malicioso | Comandos Remotos Autenticados

O sistema de informações implementa [Atribuição: salvaguardas de segurança definidas pela organização] para autenticar [Atribuição: comandos remotos definidos pela organização].  
Guia Adicional: Esse aprimoramento de controle protege contra comandos não autorizados e a reprodução de comandos autorizados. Esse recurso é importante para os sistemas de informações remotas cuja perda, mau funcionamento, desvio de direção ou exploração teria consequências imediatas e/ou graves (por exemplo, ferimentos ou morte, danos à propriedade, perda de ativos de alto valor ou informações confidenciais ou falha de informações importantes, missões / funções de negócio). As salvaguardas de autenticação para comandos remotos ajudam a garantir que os sistemas de informações aceitem e executem na ordem pretendida, apenas comandos autorizados e que comandos não autorizados sejam rejeitados. Mecanismos criptográficos podem ser empregados, por exemplo, para autenticar comandos remotos.

### SI-3(10): Proteção contra Código Malicioso | Análise de Códigos Maliciosos

A organização:  
  
a. Emprega [Atribuição: ferramentas e técnicas definidas pela organização] para analisar as características e o comportamento do código malicioso; e  
  
b. Incorpora os resultados da análise de código malicioso nos processos de resposta a incidentes organizacionais e de correção de falhas.  
Guia Adicional: A aplicação de ferramentas e técnicas de análise de código mal-intencionadas selecionadas fornece às organizações uma compreensão mais aprofundada da arte do adversário (ou seja, táticas, técnicas e procedimentos) e a funcionalidade e o objetivo de instâncias específicas de código mal-intencionado. A compreensão das características do código malicioso facilita respostas organizacionais mais eficazes a ameaças atuais e futuras. As organizações podem realizar análises maliciosas de código usando técnicas de engenharia reversa ou monitorando o comportamento de execução de código.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-83 | https://csrc.nist.gov/publications/search?keywords-lg=800-83 |

## SI-4: Monitoramento do Sistema de Informação (P1)

**Descrição do Controle:**A organização:  
  
a. Monitora o sistema de informação para detectar:  
  
1. Ataques e indicadores de possíveis ataques de acordo com [Atribuição: objetivos de monitoramento definidos pela organização]; e  
  
2. Conexões locais, de rede e remotas não autorizadas;  
  
b. Identifica o uso não autorizado do sistema de informação através de [Tarefa: técnicas e métodos definidos pela organização];  
  
c. Implanta dispositivos de monitoramento:  
  
1. Estrategicamente no sistema de informações para coletar informações essenciais determinadas pela organização; e  
  
2. Em locais ad hoc dentro do sistema para rastrear tipos específicos de transações de interesse da organização;  
  
d. Protege as informações obtidas das ferramentas de monitoramento de intrusão contra acesso, modificação e exclusão não autorizada;  
  
e. Aumenta o nível de atividade de monitoramento do sistema de informação sempre que houver uma indicação de risco aumentado para operações e ativos organizacionais, indivíduos, outras organizações ou a Nação com base em informações policiais, informações de inteligência ou outras fontes credíveis de informação;  
  
f. Obtém opinião legal em relação às atividades de monitoramento do sistema de informações, de acordo com as leis federais, ordens executivas, diretrizes, políticas ou regulamentos federais aplicáveis; e  
  
g. Fornece [Atribuição: informações de monitoramento do sistema de informações definidas pela organização] a [Atribuição: pessoal ou funções definidas pela organização] [Seleção (uma ou mais): conforme necessário; [Tarefa: frequência definida pela organização]].  
  
**Guia Adicional:**O monitoramento do sistema de informação inclui monitoramento externo e interno. O monitoramento externo inclui a observação de eventos que ocorrem no limite do sistema de informação (isto é, parte da defesa do perímetro e da proteção do limite). O monitoramento interno inclui a observação de eventos que ocorrem no sistema de informação. As organizações podem monitorar sistemas de informação, por exemplo, observando atividades de auditoria em tempo real ou observando outros aspectos do sistema, como padrões de acesso, características de acesso e outras ações. Os objetivos do monitoramento podem orientar a determinação dos eventos. A capacidade de monitoramento do sistema de informação é obtida por meio de uma variedade de ferramentas e técnicas (por exemplo, sistemas de detecção de intrusão, sistemas de prevenção de intrusão, software de proteção de código malicioso, ferramentas de varredura, software de monitoramento de registros de auditoria, software de monitoramento de rede). Os locais estratégicos para dispositivos de monitoramento incluem, por exemplo, locais de perímetro selecionados e farms de servidores próximos que suportam aplicativos críticos, sendo esses dispositivos normalmente empregados nas interfaces gerenciadas associadas aos controles SC-7 e AC-17. Os dispositivos de monitoramento de rede Einstein do Departamento de Segurança Interna também podem ser incluídos como dispositivos de monitoramento. A granularidade das informações de monitoramento coletadas é baseada nos objetivos de monitoramento organizacional e na capacidade dos sistemas de informação de suportar esses objetivos. Tipos específicos de transações de interesse incluem, por exemplo, tráfego HTTP (Hyper Text Transfer Protocol) que ignora proxies HTTP. O monitoramento do sistema de informações é parte integrante dos programas organizacionais de monitoramento contínuo e de resposta a incidentes. A saída do monitoramento do sistema serve como entrada para os programas de monitoramento contínuo e resposta a incidentes. Uma conexão de rede é qualquer conexão com um dispositivo que se comunica através de uma rede (por exemplo, rede local, Internet). Uma conexão remota é qualquer conexão com um dispositivo que se comunica através de uma rede externa (por exemplo, a Internet). As conexões locais, de rede e remotas podem ser com ou sem fio.  
  
**Melhorias do Controle:**

### SI-4(1): Monitoramento do Sistema de Informação | Sistema de Detecção de Introdução em Todo o Sistema

A organização conecta e configura ferramentas individuais de detecção de intrusão em um sistema de detecção de intrusão em todo o sistema de informações.

### SI-4(2): Monitoramento do Sistema de Informação | Ferramentas Automatizadas para Análise em Tempo Real

A organização emprega ferramentas automatizadas para dar suporte à análise de eventos quase em tempo real.  
Guia Adicional: As ferramentas automatizadas incluem, por exemplo, ferramentas de monitoramento de eventos com base em host, em rede, em transporte ou em armazenamento ou tecnologias de Security Information and Event Management (SIEM) que fornecem análise em tempo real de alertas e/ou notificações gerados pela organização. sistemas de informação.

### SI-4(3): Monitoramento do Sistema de Informação | Integração Automatizada de Ferramentas

A organização emprega ferramentas automatizadas para integrar ferramentas de detecção de intrusão nos mecanismos de controle de acesso e controle de fluxo, para uma rápida resposta a ataques, permitindo a reconfiguração desses mecanismos em apoio ao isolamento e eliminação de ataques.

### SI-4(4): Monitoramento do Sistema de Informação | Tráfego de Comunicações Inbound e Outbound

O sistema de informações monitora o tráfego de comunicações de entrada e saída [Atribuição: frequência definida pela organização] para atividades ou condições incomuns ou não autorizadas.  
Guia Adicional: As atividades ou condições incomuns / não autorizadas relacionadas ao tráfego de comunicações de entrada e saída do sistema de informação incluem, por exemplo, tráfego interno que indica a presença de código malicioso nos sistemas de informações organizacionais ou propagação entre componentes do sistema, exportação não autorizada de informações ou sinalização para informações externas sistemas. A evidência de código malicioso é usada para identificar sistemas de informações ou componentes de sistema potencialmente comprometidos.

### SI-4(5): Monitoramento do Sistema de Informação | Alertas Gerados pelo Sistema

O sistema de informações alerta [Designação: pessoal ou funções definidas pela organização] quando ocorrem as seguintes indicações de comprometimento ou possível comprometimento: [Designação: indicadores de comprometimento definido pela organização].  
Guia Adicional: Os alertas podem ser gerados a partir de uma variedade de fontes, incluindo, por exemplo, registros ou entradas de auditoria de mecanismos maliciosos de proteção de código, mecanismos de detecção ou prevenção de intrusões ou dispositivos de proteção de limites, como firewalls, gateways e roteadores. Os alertas podem ser transmitidos, por exemplo, por telefone, por mensagens de correio eletrônico ou por mensagens de texto. O pessoal da organização na lista de notificações pode incluir, por exemplo, administradores de sistemas, proprietários de missões / empresas, proprietários de sistemas ou agentes de segurança do sistema de informações.

### SI-4(6): Monitoramento do Sistema de Informação | Usuários Restritos não Privilegiados

[Retirado: Incorporado ao AC-6 (10)].

### SI-4(7): Monitoramento do Sistema de Informação | Resposta Automatizada a Eventos Suspeitos

O sistema de informações notifica [Atribuição: equipe de resposta a incidentes definida pela organização (identificada por nome e/ou função)] dos eventos suspeitos detectados e realiza [Atribuição: ações menos disruptivas definidas pela organização para encerrar eventos suspeitos].  
Guia Adicional: Ações menos perturbadoras podem incluir, por exemplo, iniciar solicitações de respostas humanas.

### SI-4(8): Monitoramento do Sistema de Informação | Proteção de Informação de Monitoramento

[Retirado: Incorporado no SI-4].

### SI-4(9): Monitoramento do Sistema de Informação | Teste de Ferramentas de Monitoramento

A organização testa ferramentas de monitoramento de intrusão [Atribuição: frequência definida pela organização].  
Guia Adicional: O teste das ferramentas de monitoramento de intrusão é necessário para garantir que as ferramentas estejam funcionando corretamente e continuem a atender aos objetivos de monitoramento das organizações. A frequência dos testes depende dos tipos de ferramentas usadas pelas organizações e dos métodos de implantação.

### SI-4(10): Monitoramento do Sistema de Informação | Visibilidade de Comunicações Criptografadas

A organização faz provisões para que [Atribuição: tráfego de comunicações criptografadas definidas pela organização] fique visível para [Atribuição: ferramentas de monitoramento do sistema de informações definidas pela organização].  
Guia Adicional: As organizações equilibram as necessidades potencialmente conflitantes de criptografar o tráfego de comunicações e de obter informações sobre esse tráfego de uma perspectiva de monitoramento. Para algumas organizações, a necessidade de garantir a confidencialidade do tráfego de comunicações é fundamental; para outros, a garantia da missão é uma preocupação maior. As organizações determinam se o requisito de visibilidade se aplica ao tráfego criptografado interno, ao tráfego criptografado destinado a destinos externos ou a um subconjunto dos tipos de tráfego.

### SI-4(11): Monitoramento do Sistema de Informação | Analisar Anomalias de Tráfego de Comunicações

A organização analisa o tráfego de comunicações de saída nos limites externos do sistema de informação e seleciona [Atribuição: pontos internos definidos pela organização no sistema (por exemplo, sub-redes, subsistemas)] para descobrir anomalias.  
Guia Adicional: As anomalias nos sistemas de informações organizacionais incluem, por exemplo, grandes transferências de arquivos, conexões persistentes de longa data, protocolos e portas incomuns em uso e tentativa de comunicação com suspeitos de endereços externos maliciosos.

### SI-4(12): Monitoramento do Sistema de Informação | Alertas Automatizados

A organização emprega mecanismos automatizados para alertar a equipe de segurança sobre as seguintes atividades inadequadas ou incomuns com implicações na segurança: [Atribuição: atividades definidas pela organização que acionam alertas].  
Guia Adicional: Esse aprimoramento de controle se concentra nos alertas de segurança gerados pelas organizações e transmitidos por meios automatizados. Ao contrário dos alertas gerados pelos sistemas de informação no SI-4 (5), que tendem a se concentrar em fontes de informação internas aos sistemas (por exemplo, registros de auditoria), as fontes de informação para esse aprimoramento também podem incluir outras entidades (por exemplo, , relatórios de atividades suspeitas, relatórios sobre possíveis ameaças internas).

### SI-4(13): Monitoramento do Sistema de Informação | Analisar Padrões de Tráfego / Evento

A organização:  
  
a. Analisa padrões de tráfego / evento de comunicações para o sistema de informação;  
  
b. Desenvolve perfis que representam padrões e/ou eventos de tráfego comuns; e  
  
c. Usa os perfis de tráfego / evento nos dispositivos de monitoramento do sistema de ajuste para reduzir o número de falsos positivos e o número de falsos negativos.

### SI-4(14): Monitoramento do Sistema de Informação | Detecção de Intrusão Sem Fio

A organização emprega um sistema de detecção de intrusão sem fio para identificar dispositivos sem fio não autorizados e para detectar tentativas de ataque e possíveis comprometimentos / violações no sistema de informações.  
Guia Adicional: Os sinais sem fio podem irradiar além dos limites das instalações controladas pela organização. As organizações pesquisam proativamente conexões sem fio não autorizadas, incluindo a realização de varreduras completas de pontos de acesso sem fio não autorizados. As verificações não se limitam às áreas dentro das instalações que contêm sistemas de informação, mas também incluem áreas fora das instalações, conforme necessário, para verificar se os pontos de acesso sem fio não autorizados não estão conectados aos sistemas.

### SI-4(15): Monitoramento do Sistema de Informação | Comunicações Sem Fio para Com Fio

A organização emprega um sistema de detecção de intrusões para monitorar o tráfego de comunicações sem fio à medida que o tráfego passa das redes sem fio para as redes com fio.

### SI-4(16): Monitoramento do Sistema de Informação | Informação Correta de Monitoramento

A organização correlaciona as informações das ferramentas de monitoramento empregadas em todo o sistema de informações.  
Guia Adicional: A correlação de informações de diferentes ferramentas de monitoramento pode fornecer uma visão mais abrangente da atividade do sistema de informações. A correlação de ferramentas de monitoramento que geralmente funcionam isoladamente (por exemplo, monitoramento de host, monitoramento de rede, software antivírus) pode fornecer uma visão geral da organização e, ao fazê-lo, pode revelar padrões de ataque não vistos. Compreender os recursos / limitações de diversas ferramentas de monitoramento e como maximizar a utilidade das informações geradas por essas ferramentas pode ajudar as organizações a criar, operar e manter programas de monitoramento eficazes.

### SI-4(17): Monitoramento do Sistema de Informação | Consciência Situacional Integrada

A organização correlaciona as informações do monitoramento de atividades físicas, cibernéticas e da cadeia de suprimentos para obter consciência situacional integrada em toda a organização.  
Guia Adicional: Esse aprimoramento de controle correlaciona as informações de monitoramento de um conjunto mais diversificado de fontes de informações para obter consciência situacional integrada. A conscientização situacional integrada de uma combinação de atividades de monitoramento físico, cibernético e da cadeia de suprimentos aumenta a capacidade das organizações de detectar mais rapidamente ataques cibernéticos sofisticados e investigar os métodos e técnicas empregados para realizar esses ataques. Ao contrário do SI-4 (16), que correlaciona as várias informações de monitoramento cibernético, esse aprimoramento de controle correlaciona o monitoramento além do domínio cibernético. Esse monitoramento pode ajudar a revelar ataques a organizações que operam em vários vetores de ataque.

### SI-4(18): Monitoramento do Sistema de Informação | Analisar Tráfego / Exfiltração de Cobertura

A organização analisa o tráfego de comunicações de saída no limite externo do sistema de informação (ou seja, perímetro do sistema) e em [Atribuição: pontos internos definidos pela organização no sistema (por exemplo, subsistemas, sub-redes)] para detectar a exfiltração secreta de informações.  
Guia Adicional: Encoberto significa que pode ser usado para a exfiltração não autorizada de informações organizacionais, por exemplo, esteganografia.

### SI-4(19): Monitoramento do Sistema de Informação | Indivíduos que Possuem Maior Risco

A organização implementa [Atribuição: monitoramento adicional definido pela organização] de indivíduos que foram identificados por [Atribuição: fontes definidas pela organização] como apresentando um nível de risco aumentado.  
Guia Adicional: Indicações de aumento de risco de indivíduos podem ser obtidas de várias fontes, incluindo, por exemplo, registros de recursos humanos, agências de inteligência, organizações policiais e/ou outras fontes confiáveis. O monitoramento de indivíduos é coordenado de perto com os funcionários de gerenciamento, jurídico, segurança e recursos humanos das organizações que conduzem esse monitoramento e está em conformidade com a legislação federal, ordens executivas, políticas, diretrizes, regulamentos e normas.

### SI-4(20): Monitoramento do Sistema de Informação | Usuários Privilegiados

A organização implementa [Atribuição: monitoramento adicional definido pela organização] de usuários privilegiados.

### SI-4(21): Monitoramento do Sistema de Informação | Períodos Probativos

A organização implementa [Tarefa: monitoramento adicional definido pela organização] de indivíduos durante [Tarefa: período probatório definido pela organização].

### SI-4(22): Monitoramento do Sistema de Informação | Serviços de Rede Não Autorizados

O sistema de informações detecta serviços de rede que não foram autorizados ou aprovados por [Atribuição: autorização definida pela organização ou processos de aprovação] e [Seleção (uma ou mais): auditorias; alertas [Atribuição: pessoal ou funções definidas pela organização]].  
Guia Adicional: Serviços de rede não autorizados ou não aprovados incluem, por exemplo, serviços em arquiteturas orientadas a serviços que não possuem verificação ou validação organizacional e, portanto, podem não ser confiáveis ou servir como bandidos maliciosos para serviços válidos.

### SI-4(23): Monitoramento do Sistema de Informação | Dispositivos Baseados em Host

A organização implementa [Atribuição: mecanismos de monitoramento baseados em host definidos pela organização] em [Atribuição: componentes do sistema de informações definidos pela organização].  
Guia Adicional: Os componentes do sistema de informações onde o monitoramento baseado em host pode ser implementado incluem, por exemplo, servidores, estações de trabalho e dispositivos móveis. As organizações consideram empregar mecanismos de monitoramento baseados em host de vários desenvolvedores de produtos de tecnologia da informação.

### SI-4(24): Monitoramento do Sistema de Informação | Indicadores de Compromisso

O sistema de informação descobre, coleta, distribui e utiliza indicadores de comprometimento.  
Guia Adicional: Indicadores de compromisso (COI) são artefatos forenses de intrusões identificadas em sistemas de informações organizacionais (no nível do host ou da rede). Os COI fornecem às organizações informações valiosas sobre objetos ou sistemas de informações que foram comprometidos. Os IOCs para a descoberta de hosts comprometidos podem incluir, por exemplo, a criação de valores de chave do Registro. Os IOCs para tráfego de rede incluem, por exemplo, URL (Universal Resource Locator) ou elementos de protocolo que indicam servidores de comando e controle de malware. A rápida distribuição e adoção de COIs podem melhorar a segurança das informações, reduzindo o tempo em que os sistemas e as organizações estão vulneráveis à mesma exploração ou ataque.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-61 | https://csrc.nist.gov/publications/search?keywords-lg=800-61 |
| Publicação Especial NIST 800-83 | https://csrc.nist.gov/publications/search?keywords-lg=800-83 |
| Publicação Especial NIST 800-92 | https://csrc.nist.gov/publications/search?keywords-lg=800-92 |
| Publicação Especial NIST 800-94 | https://csrc.nist.gov/publications/search?keywords-lg=800-94 |
| Publicação Especial NIST 800-137 | https://csrc.nist.gov/publications/search?keywords-lg=800-137 |

## SI-5: Alertas, Conselhos e Diretivas de Segurança (P1)

**Descrição do Controle:**A organização:  
  
a. Recebe alertas, avisos e diretrizes de segurança do sistema de informações de [Atribuição: organizações externas definidas pela organização] continuamente;  
  
b. Gera alertas, avisos e diretrizes de segurança interna, conforme necessário;  
  
c. Divulga alertas de segurança, avisos e diretrizes para: [Seleção (uma ou mais): [Designação: pessoal ou funções definidas pela organização]; [Atribuição: elementos definidos pela organização dentro da organização]; [Atribuição: organizações externas definidas pela organização]]; e  
  
d. Implementa diretivas de segurança de acordo com os prazos estabelecidos ou notifica a organização emissora do grau de não conformidade.  
  
**Guia Adicional:**A Equipe de Prontidão de Emergência em Computador dos Estados Unidos (US-CERT) gera alertas e avisos de segurança para manter a consciência da situação em todo o governo federal. As diretivas de segurança são emitidas pelo OMB ou outras organizações designadas com a responsabilidade e autoridade para emiti-las. A conformidade com as diretivas de segurança é essencial devido à natureza crítica de muitas dessas diretivas e aos possíveis efeitos adversos imediatos nas operações e ativos organizacionais, indivíduos, outras organizações e a Nação, caso as diretivas não sejam implementadas em tempo hábil. As organizações externas incluem, por exemplo, parceiros externos de missão / negócios, parceiros da cadeia de suprimentos, provedores de serviços externos e outras organizações de mesmo nível / apoio.  
  
**Melhorias do Controle:**

### SI-5(1): Alertas, Conselhos e Diretivas de Segurança | Alertas, Alertas e Conselhos Automatizados

A organização emprega mecanismos automatizados para disponibilizar informações de alerta e consultoria de segurança em toda a organização.  
Guia Adicional: O número significativo de alterações nos sistemas de informações organizacionais e nos ambientes em que esses sistemas operam requer a disseminação de informações relacionadas à segurança a uma variedade de entidades organizacionais que têm interesse direto no sucesso de missões organizacionais e funções de negócios. Com base nas informações fornecidas pelos alertas e alertas de segurança, podem ser necessárias alterações em uma ou mais das três camadas relacionadas ao gerenciamento de riscos à segurança da informação, incluindo o nível de governança, missão / processos de negócios / arquitetura corporativa e o sistema de informações nível.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-40 | https://csrc.nist.gov/publications/search?keywords-lg=800-40 |

## SI-6: Verificação da Função de Segurança (P1)

**Descrição do Controle:**O sistema de informação:  
  
a. Verifica a operação correta de [Atribuição: funções de segurança definidas pela organização];  
  
b. Executa esta verificação [Seleção (uma ou mais): [Atribuição: estados transitórios do sistema definido pela organização]; sob comando do usuário com privilégio apropriado; [Tarefa: frequência definida pela organização]];  
  
c. Notifica [Atribuição: pessoal ou funções definidas pela organização] de falhas nos testes de verificação de segurança; e  
  
d. [Seleção (uma ou mais): desliga o sistema de informação; reinicia o sistema de informação; [Atribuição: ação (s) alternativa (s) definida (s) pela organização]] quando anomalias são descobertas.  
  
**Guia Adicional:**Os estados de transição para sistemas de informação incluem, por exemplo, inicialização, reinicialização, encerramento e abortamento do sistema. As notificações fornecidas pelos sistemas de informação incluem, por exemplo, alertas eletrônicos para os administradores do sistema, mensagens para os consoles do computador local e/ou indicações de hardware, como luzes.  
  
**Melhorias do Controle:**

### SI-6(1): Verificação da Função de Segurança | Notificação de Ensaios de Segurança Falhados

[Retirado: Incorporado no SI-6].

### SI-6(2): Verificação da Função de Segurança | Suporte de Automação para Testes Distribuídos

O sistema de informações implementa mecanismos automatizados para dar suporte ao gerenciamento de testes de segurança distribuídos.

### SI-6(3): Verificação da Função de Segurança | Relatório Resultados da Verificação

A organização reporta os resultados da verificação da função de segurança para [Atribuição: pessoal ou funções definidas pela organização].  
Guia Adicional: O pessoal da organização com potencial interesse nos resultados da verificação das funções de segurança inclui, por exemplo, oficiais seniores de segurança da informação, gerentes de segurança do sistema de informação e oficiais de segurança do sistema de informação.

## SI-7: Integridade de Software, Firmware e Informação (P1)

**Descrição do Controle:**A organização emprega ferramentas de verificação de integridade para detectar alterações não autorizadas em [Atribuição: software, firmware e informações definidos pela organização].  
  
**Guia Adicional:**Alterações não autorizadas no software, firmware e informações podem ocorrer devido a erros ou atividades maliciosas (por exemplo, adulteração). O software inclui, por exemplo, sistemas operacionais (com os principais componentes internos, como kernels, drivers), middleware e aplicativos. O firmware inclui, por exemplo, o BIOS (Basic Input Output System). As informações incluem metadados, como atributos de segurança associados às informações. Mecanismos de verificação de integridade de última geração (por exemplo, verificações de paridade, verificações cíclicas de redundância, hashes criptográficos) e ferramentas associadas podem monitorar automaticamente a integridade dos sistemas de informação e aplicativos hospedados.  
  
**Melhorias do Controle:**

### SI-7(1): Integridade de Software, Firmware e Informação | Integridade de Software, Verificações da Integridade

O sistema de informações executa uma verificação de integridade de [Atribuição: software, firmware e informações definidos pela organização] [Seleção (uma ou mais): na inicialização; em [Atribuição: estados transitórios definidos pela organização ou eventos relevantes à segurança]; [Tarefa: frequência definida pela organização]].  
Guia Adicional: Os eventos relevantes para a segurança incluem, por exemplo, a identificação de uma nova ameaça à qual os sistemas de informações organizacionais são suscetíveis e a instalação de novo hardware, software ou firmware. Os estados de transição incluem, por exemplo, inicialização do sistema, reinicialização, desligamento e anulação.

### SI-7(2): Integridade de Software, Firmware e Informação | Integridade de Software, Notificações Automatizadas de Violações de Integridade

A organização emprega ferramentas automatizadas que notificam [Atribuição: pessoal ou funções definidas pela organização] ao descobrir discrepâncias durante a verificação de integridade.  
Guia Adicional: O uso de ferramentas automatizadas para relatar violações de integridade e para notificar o pessoal da organização em tempo hábil é um precursor essencial para uma resposta eficaz aos riscos. O pessoal interessado em violações da integridade inclui, por exemplo, proprietários de missão / empresa, proprietários de sistemas de informação, administradores de sistemas, desenvolvedores de software, integradores de sistemas e agentes de segurança da informação.

### SI-7(3): Integridade de Software, Firmware e Informação | Integridade de Software, Ferramentas de Integridade Gerenciadas Centralmente

A organização emprega ferramentas de verificação de integridade gerenciadas centralmente.

### SI-7(4): Integridade de Software, Firmware e Informação | Integridade de Software, Embalagem Evidente

[Retirado: Incorporado na SA-12].

### SI-7(5): Integridade de Software, Firmware e Informação | Integridade de Software, Resposta Automatizada a Violações de Integridade

O sistema de informação automaticamente [Seleção (uma ou mais): desliga o sistema de informação; reinicia o sistema de informação; implementa [Atribuição: salvaguardas de segurança definidas pela organização]] quando violações de integridade são descobertas.  
Guia Adicional: As organizações podem definir diferentes verificações de integridade e respostas a anomalias: (i) por tipo de informação (por exemplo, firmware, software, dados do usuário); (ii) por informações específicas (por exemplo, firmware de inicialização, firmware de inicialização para tipos específicos de máquinas); ou (iii) uma combinação de ambos. A implementação automática de salvaguardas específicas nos sistemas de informações organizacionais inclui, por exemplo, reverter as alterações, interromper o sistema de informações ou acionar alertas de auditoria quando ocorrem modificações não autorizadas nos arquivos críticos de segurança.

### SI-7(6): Integridade de Software, Firmware e Informação | Integridade de Software, Proteção Criptográfica

O sistema de informações implementa mecanismos criptográficos para detectar alterações não autorizadas no software, firmware e informações.  
Guia Adicional: Os mecanismos criptográficos usados para a proteção da integridade incluem, por exemplo, assinaturas digitais e o cálculo e aplicação de hashes assinados usando criptografia assimétrica, protegendo a confidencialidade da chave usada para gerar o hash e usando a chave pública para verificar as informações do hash.

### SI-7(7): Integridade de Software, Firmware e Informação | Integridade de Software, Integração de Detecção e Resposta

A organização incorpora a detecção de [Atribuição: alterações relevantes à segurança definidas pela organização no sistema de informações] no recurso de resposta a incidentes da organização.  
Guia Adicional: Esse aprimoramento de controle ajuda a garantir que os eventos detectados sejam rastreados, monitorados, corrigidos e disponíveis para fins históricos. A manutenção de registros históricos é importante para poder identificar e discernir ações adversas por um longo período de tempo e para possíveis ações legais. As alterações relevantes à segurança incluem, por exemplo, alterações não autorizadas nas definições de configuração estabelecidas ou elevação não autorizada de privilégios do sistema de informações.

### SI-7(8): Integridade de Software, Firmware e Informação | Integridade de Software, Capacidade de Auditoria em Eventos Significativos

O sistema de informações, ao detectar uma possível violação de integridade, fornece a capacidade de auditar o evento e inicia as seguintes ações: [Seleção (uma ou mais): gera um registro de auditoria; alerta o usuário atual; alertas [Atribuição: pessoal ou funções definidas pela organização]; [Tarefa: outras ações definidas pela organização]].  
Guia Adicional: As organizações selecionam ações de resposta com base em tipos de software, software específico ou informações para as quais existem possíveis violações de integridade.

### SI-7(9): Integridade de Software, Firmware e Informação | Integridade de Software, Verificar o Processo de Inicialização

O sistema de informações verifica a integridade do processo de inicialização de [Atribuição: dispositivos definidos pela organização].  
Guia Adicional: Garantir a integridade dos processos de inicialização é fundamental para iniciar dispositivos em estados conhecidos / confiáveis. Os mecanismos de verificação de integridade fornecem à equipe organizacional a garantia de que apenas o código confiável é executado durante os processos de inicialização.

### SI-7(10): Integridade de Software, Firmware e Informação | Integridade de Software, Proteção do Firmware de Boot

O sistema de informações implementa [Atribuição: salvaguardas de segurança definidas pela organização] para proteger a integridade do firmware de inicialização em [Atribuição: dispositivos definidos pela organização].  
Guia Adicional: Modificações não autorizadas no firmware de inicialização podem ser indicativas de um ataque cibernético sofisticado e direcionado. Esses tipos de ataques cibernéticos podem resultar em uma negação de serviço permanente (por exemplo, se o firmware estiver corrompido) ou em uma presença persistente de código malicioso (por exemplo, se o código estiver incorporado no firmware). Os dispositivos podem proteger a integridade do firmware de inicialização nos sistemas de informações organizacionais: (i) verificando a integridade e a autenticidade de todas as atualizações do firmware de inicialização antes de aplicar alterações nos dispositivos de inicialização; e (ii) impedir que processos não autorizados modifiquem o firmware de inicialização.

### SI-7(11): Integridade de Software, Firmware e Informação | Integridade de Software, Ambientes Confinados com Privilégios Limitados

A organização exige que [Atribuição: software instalado pelo usuário definido pela organização] seja executado em um ambiente de máquina física ou virtual confinada com privilégios limitados.  
Guia Adicional: As organizações identificam software que pode ser uma preocupação maior em relação à origem ou ao potencial de conter código malicioso. Para esse tipo de software, as instalações do usuário ocorrem em ambientes confinados de operação para limitar ou conter danos causados por códigos maliciosos que podem ser executados.

### SI-7(12): Integridade de Software, Firmware e Informação | Integridade de Software, Verificação da Integridade

A organização exige que a integridade do [Atribuição: software instalado pelo usuário definido pela organização] seja verificada antes da execução.  
Guia Adicional: As organizações verificam a integridade do software instalado pelo usuário antes da execução para reduzir a probabilidade de execução de códigos maliciosos ou códigos que contenham erros de modificações não autorizadas. As organizações consideram a praticidade de abordagens para verificar a integridade do software, incluindo, por exemplo, disponibilidade de somas de verificação com confiabilidade adequada por desenvolvedores ou fornecedores de software.

### SI-7(13): Integridade de Software, Firmware e Informação | Integridade de Software, Execução de Código em Ambientes Protegidos

A organização permite a execução de código binário ou executável por máquina obtido de fontes com garantia limitada ou inexistente e sem o fornecimento de código-fonte apenas em ambientes físicos ou de máquinas virtuais confinados e com a aprovação explícita de [Atribuição: funções ou pessoal definido pela organização] .  
Guia Adicional: Esse aprimoramento de controle se aplica a todas as fontes de código binário ou executável por máquina, incluindo, por exemplo, software / firmware comercial e software de código aberto.

### SI-7(14): Integridade de Software, Firmware e Informação | Integridade de Software, Código Executável Binário Ou Máquina

A organização:  
  
a. Proíbe o uso de código binário ou executável por máquina de fontes com garantia limitada ou nenhuma e sem o fornecimento de código-fonte; e  
  
b. Fornece exceções ao requisito do código-fonte somente para requisitos operacionais / de missão convincentes e com a aprovação do autorizador.  
Guia Adicional: Esse aprimoramento de controle se aplica a todas as fontes de código binário ou executável por máquina, incluindo, por exemplo, software / firmware comercial e software de código aberto. As organizações avaliam produtos de software sem o código fonte de fontes com garantia limitada ou inexistente para possíveis impactos à segurança. As avaliações abordam o fato de que esses tipos de produtos de software podem ser muito difíceis de revisar, reparar ou estender, uma vez que as organizações, na maioria dos casos, não têm acesso ao código fonte original e pode não haver proprietários que possam fazer isso. esses reparos em nome das organizações.

### SI-7(15): Integridade de Software, Firmware e Informação | Integridade de Software, Autenticação de Código

O sistema de informações implementa mecanismos criptográficos para autenticar [Atribuição: software definido pela organização ou componentes de firmware] antes da instalação.  
Guia Adicional: A autenticação criptográfica inclui, por exemplo, a verificação de que os componentes de software ou firmware foram assinados digitalmente usando certificados reconhecidos e aprovados pelas organizações. A assinatura de código é um método eficaz de proteção contra códigos maliciosos.

### SI-7(16): Integridade de Software, Firmware e Informação | Integridade de Software, Prazo de Execução do Processo Sem Supervisão

A organização não permite que os processos sejam executados sem supervisão por mais de [Atribuição: período definido pela organização].  
Guia Adicional: Esse aprimoramento de controle aborda processos para os quais períodos normais de execução podem ser determinados e situações em que as organizações excedem esses períodos. A supervisão inclui, por exemplo, temporizadores do sistema operacional, respostas automatizadas ou supervisão e resposta manuais quando ocorrem anomalias no processo do sistema de informação.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-147 | https://csrc.nist.gov/publications/search?keywords-lg=800-147 |
| Publicação Especial NIST 800-155 | https://csrc.nist.gov/publications/search?keywords-lg=800-155 |

## SI-8: Proteção Contra Spam (P2)

**Descrição do Controle:**A organização:  
  
a. Emprega mecanismos de proteção contra spam nos pontos de entrada e saída do sistema de informações para detectar e executar ações em mensagens não solicitadas; e  
  
b. Atualiza os mecanismos de proteção contra spam quando novas versões estão disponíveis, de acordo com a política e os procedimentos de gerenciamento de configuração organizacional.  
  
**Guia Adicional:**Os pontos de entrada e saída do sistema de informação incluem, por exemplo, firewalls, servidores de correio eletrônico, servidores Web, servidores proxy, servidores de acesso remoto, estações de trabalho, dispositivos móveis e notebooks / laptops. O spam pode ser transportado por diferentes meios, incluindo, por exemplo, correio eletrônico, anexos de correio eletrônico e acessos à Web. Os mecanismos de proteção contra spam incluem, por exemplo, definições de assinatura.  
  
**Melhorias do Controle:**

### SI-8(1): Proteção Contra Spam | Gestão Central

A organização gerencia centralmente os mecanismos de proteção contra spam.  
Guia Adicional: Gerenciamento central é o gerenciamento e implementação de mecanismos de proteção contra spam em toda a organização. O gerenciamento central inclui planejar, implementar, avaliar, autorizar e monitorar os controles de segurança de proteção contra spam, definidos pela organização e gerenciados centralmente.

### SI-8(2): Proteção Contra Spam | Atualizações Automáticas

O sistema de informações atualiza automaticamente os mecanismos de proteção contra spam.

### SI-8(3): Proteção Contra Spam | Capacidade de Aprendizagem Contínua

O sistema de informações implementa mecanismos de proteção contra spam com capacidade de aprendizado para identificar com mais eficiência o tráfego legítimo de comunicações.  
Guia Adicional: Os mecanismos de aprendizado incluem, por exemplo, filtros bayesianos que respondem às entradas do usuário identificando tráfego específico como spam ou legítimo, atualizando os parâmetros do algoritmo e, assim, separando com mais precisão os tipos de tráfego.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-45 | https://csrc.nist.gov/publications/search?keywords-lg=800-45 |

## SI-9: Restrições de Entrada de Informação (P0)

**Descrição do Controle:**[Retirado: Incorporado em AC-2, AC-3, AC-5, AC-6].

## SI-10: Validação de Entrada de Informação (P1)

**Descrição do Controle:**O sistema de informações verifica a validade de [Atribuição: entradas de informações definidas pela organização].  
  
**Guia Adicional:**A verificação da sintaxe e da semântica válidas das entradas do sistema de informações (por exemplo, conjunto de caracteres, comprimento, intervalo numérico e valores aceitáveis) verifica se as entradas correspondem às definições especificadas para formato e conteúdo. Os aplicativos de software geralmente seguem protocolos bem definidos que usam mensagens estruturadas (isto é, comandos ou consultas) para se comunicar entre módulos de software ou componentes do sistema. As mensagens estruturadas podem conter dados brutos ou não estruturados, intercalados com metadados ou informações de controle. Se os aplicativos de software usarem entradas fornecidas pelo invasor para construir mensagens estruturadas sem codificá-las adequadamente, o invasor poderá inserir comandos maliciosos ou caracteres especiais que possam fazer com que os dados sejam interpretados como informações de controle ou metadados. Consequentemente, o módulo ou componente que recebe a saída contaminada executará as operações incorretas ou interpretará os dados incorretamente. A pré-seleção das entradas antes da passagem para os intérpretes impede que o conteúdo seja intencionalmente interpretado como comandos. A validação de entrada ajuda a garantir entradas precisas e corretas e a evitar ataques como scripts entre sites e uma variedade de ataques de injeção.  
  
**Melhorias do Controle:**

### SI-10(1): Validação de Entrada de Informação | Capacidade de Substituição Manual

O sistema de informação:  
  
a. Fornece um recurso de substituição manual para validação de entrada de [Atribuição: entradas definidas pela organização];  
  
b. Restringe o uso do recurso de substituição manual apenas para [Atribuição: indivíduos autorizados definidos pela organização]; e  
  
c. Audita o uso do recurso de substituição manual.

### SI-10(2): Validação de Entrada de Informação | Revisão/Resolução de Erros

A organização garante que os erros de validação de entrada sejam revisados e resolvidos dentro de [Atribuição: período definido pela organização].  
Guia Adicional: A resolução de erros de validação de entrada inclui, por exemplo, a correção de causas sistêmicas de erros e o reenvio de transações com entrada corrigida.

### SI-10(3): Validação de Entrada de Informação | Comportamento Previsível

O sistema de informações se comporta de maneira previsível e documentada que reflete os objetivos organizacionais e do sistema quando entradas inválidas são recebidas.  
Guia Adicional: Uma vulnerabilidade comum nos sistemas de informações organizacionais é um comportamento imprevisível quando entradas inválidas são recebidas. Esse aprimoramento de controle garante que haja um comportamento previsível diante de entradas inválidas, especificando respostas do sistema de informações que facilitam a transição do sistema para estados conhecidos sem efeitos colaterais indesejados e indesejados.

### SI-10(4): Validação de Entrada de Informação | Interações de Revisão/Tempo

A organização contabiliza as interações de tempo entre os componentes do sistema de informações na determinação de respostas apropriadas para entradas inválidas.  
Guia Adicional: Ao abordar entradas inválidas do sistema de informações recebidas nas interfaces de protocolo, as interações de temporização se tornam relevantes, onde um protocolo precisa considerar o impacto da resposta a erros em outros protocolos na pilha de protocolos. Por exemplo, os protocolos de rede sem fio padrão 802.11 não interagem bem com os protocolos de controle de transmissão (TCP) quando os pacotes são descartados (o que pode ocorrer devido à entrada de pacotes inválida). O TCP supõe que as perdas de pacotes sejam devidas ao congestionamento, enquanto os pacotes perdidos nos links 802.11 geralmente são descartados devido a colisões ou ruídos no link. Se o TCP der uma resposta de congestionamento, será executada com precisão a ação errada em resposta a um evento de colisão. Os adversários podem ser capazes de usar comportamentos individuais aparentemente aceitáveis dos protocolos em conjunto para obter efeitos adversos através da construção adequada de informações inválidas.

### SI-10(5): Validação de Entrada de Informação | Entradas Restritas a Fontes Confiáveis e Formatos Aprovados

A organização restringe o uso de informações para [Atribuição: fontes confiáveis definidas pela organização] e/ou [Atribuição: formatos definidos pela organização].  
Guia Adicional: Esse aprimoramento de controle aplica o conceito de lista de permissões às entradas de informações. A especificação de fontes confiáveis conhecidas para entradas de informações e formatos aceitáveis para essas entradas pode reduzir a probabilidade de atividade maliciosa.

## SI-11: Controle de Erros (P2)

**Descrição do Controle:**O sistema de informação:  
  
a. Gera mensagens de erro que fornecem informações necessárias para ações corretivas sem revelar informações que poderiam ser exploradas por adversários; e  
  
b. Revela mensagens de erro apenas para [Atribuição: pessoal ou funções definidas pela organização].  
  
**Guia Adicional:**As organizações consideram cuidadosamente a estrutura / conteúdo das mensagens de erro. A extensão em que os sistemas de informação são capazes de identificar e lidar com condições de erro é guiada pela política organizacional e pelos requisitos operacionais. As informações que podem ser exploradas pelos adversários incluem, por exemplo, tentativas incorretas de login com senhas inseridas por engano como nome de usuário, informações de missão / negócios que podem ser derivadas de (se não declaradas explicitamente por) informações registradas e informações pessoais, como números de contas, números de previdência social e números de cartão de crédito. Além disso, as mensagens de erro podem fornecer um canal secreto para a transmissão de informações.

## SI-12: Manuseio e Controle de Informações (P2)

**Descrição do Controle:**A organização lida e retém as informações no sistema de informações e a saída de informações do sistema, de acordo com as leis federais aplicáveis, ordens executivas, diretrizes, políticas, regulamentos, padrões e requisitos operacionais.  
  
**Guia Adicional:**Os requisitos de manipulação e retenção de informações abrangem todo o ciclo de vida das informações, em alguns casos estendendo-se além da disposição dos sistemas de informação. A Administração Nacional de Arquivos e Registros fornece orientações sobre a retenção de registros.

## SI-13: Prevenção de Falhas Previsíveis (P0)

**Descrição do Controle:**A organização:  
  
a. Determina o tempo médio até a falha (MTTF) para [Atribuição: componentes do sistema de informações definidos pela organização] em ambientes específicos de operação; e  
  
b. Fornece componentes de sistema de informação substitutos e um meio para trocar componentes ativos e em espera em [Atribuição: critérios de substituição de MTTF definidos pela organização].  
  
**Guia Adicional:**Embora o MTTF seja principalmente um problema de confiabilidade, esse controle aborda possíveis falhas de componentes específicos do sistema de informações que fornecem capacidade de segurança. As taxas de falha refletem considerações específicas da instalação, e não a média da indústria. As organizações definem critérios para a substituição de componentes do sistema de informações com base no valor do MTTF, levando em consideração os possíveis danos resultantes de falhas nos componentes. A transferência de responsabilidades entre componentes ativos e em espera não compromete a segurança, a prontidão operacional ou a capacidade de segurança (por exemplo, preservação de variáveis de estado). Os componentes em espera permanecem disponíveis o tempo todo, exceto por problemas de manutenção ou falhas de recuperação em andamento.  
  
**Melhorias do Controle:**

### SI-13(1): Prevenção de Falhas Previsíveis | Transferindo Responsabilidades de Componentes

A organização coloca fora de serviço os componentes do sistema de informações, transferindo as responsabilidades dos componentes para substituí-los o mais tardar em [Atribuição: fração ou porcentagem definida pela organização] do tempo médio até a falha.

### SI-13(2): Prevenção de Falhas Previsíveis | Prazo de Execução do Processo Sem Supervisão

[Retirado: Incorporado no SI-7 (16)].

### SI-13(3): Prevenção de Falhas Previsíveis | Transferência Manual Entre Componentes

A organização inicia manualmente as transferências entre os componentes do sistema de informações ativo e em espera [Atribuição: frequência definida pela organização] se o tempo médio até a falha exceder [Atribuição: período definido pela organização].

### SI-13(4): Prevenção de Falhas Previsíveis | Instalação/Notificação de Componente Standby

A organização, se forem detectadas falhas no componente do sistema de informações:  
  
a. Garante que os componentes em espera sejam instalados com êxito e de forma transparente dentro de [Atribuição: período definido pela organização]; e  
  
b. [Seleção (uma ou mais): ativa [Atribuição: alarme definido pela organização]; desliga automaticamente o sistema de informação].  
Guia Adicional: A transferência automática ou manual de componentes do modo de espera para o ativo pode ocorrer, por exemplo, na detecção de falhas de componentes.

### SI-13(5): Prevenção de Falhas Previsíveis | Falha na Capacidade

A organização fornece [Seleção: em tempo real; quase em tempo real] [Atribuição: recurso de failover definido pela organização] para o sistema de informações.  
Guia Adicional: O failover refere-se à alternância automática para um sistema de informações alternativo após a falha do sistema de informações primário. O recurso de failover inclui, por exemplo, incorporar operações do sistema de informações espelhadas em sites de processamento alternativos ou espelhamento periódico de dados em intervalos regulares definidos pelos períodos de recuperação das organizações.

## SI-14: Não-Persistência (P0)

**Descrição do Controle:**A organização implementa [Atribuição: componentes e serviços do sistema de informações definidos pela organização] não persistentes que são iniciados em um estado conhecido e finalizados [Seleção (um ou mais): ao final da sessão de uso; periodicamente em [Tarefa: frequência definida pela organização]].  
  
**Guia Adicional:**Esse controle reduz o risco de ameaças persistentes avançadas (APTs), reduzindo significativamente a capacidade de direcionamento dos adversários (isto é, janela de oportunidade e superfície de ataque disponível) para iniciar e concluir ataques cibernéticos. Ao implementar o conceito de não persistência para componentes selecionados do sistema de informações, as organizações podem fornecer um recurso de computação de estado conhecido por um período específico de tempo que não dê aos adversários tempo suficiente no alvo para explorar vulnerabilidades nos sistemas de informações organizacionais e nos ambientes nos quais esses sistemas operam. Como a ameaça persistente avançada é uma ameaça de alto nível em relação à capacidade, intenção e direcionamento, as organizações assumem que, por um período prolongado, uma porcentagem de ataques cibernéticos será bem-sucedida. Os componentes e serviços do sistema de informações não persistentes são ativados conforme necessário usando informações protegidas e finalizados periodicamente ou no final das sessões. A não persistência aumenta o fator de trabalho dos adversários na tentativa de comprometer ou violar os sistemas de informações organizacionais. Componentes do sistema não persistentes podem ser implementados, por exemplo, periodicamente com a criação de novas imagens de componentes ou usando uma variedade de técnicas comuns de virtualização. Os serviços não persistentes podem ser implementados usando técnicas de virtualização como parte de máquinas virtuais ou como novas instâncias de processos em máquinas físicas (persistentes ou não persistentes). O benefício de atualizações periódicas dos componentes / serviços do sistema de informação é que ele não requer organizações para determinar primeiro se houve comprometimento de componentes ou serviços (algo que pode ser difícil para as organizações determinar). A atualização dos componentes e serviços selecionados do sistema de informações ocorre com frequência suficiente para impedir a propagação ou o impacto pretendido dos ataques, mas não com a frequência que torna o sistema de informações instável. Em alguns casos, atualizações de componentes e serviços críticos podem ser feitas periodicamente, a fim de impedir a capacidade dos adversários de explorar janelas ideais de vulnerabilidades.  
  
**Melhorias do Controle:**

### SI-14(1): Não-Persistência | Atualização de Fontes Confiáveis

A organização garante que o software e os dados empregados durante as atualizações de componentes e serviços do sistema de informações sejam obtidos em [Atribuição: fontes confiáveis definidas pela organização].  
Guia Adicional: As fontes confiáveis incluem, por exemplo, software / dados de mídia de gravação única, somente leitura ou de instalações de armazenamento seguras off-line selecionadas.

## SI-15: Filtro de Saída de Informação (P0)

**Descrição do Controle:**O sistema de informações valida a saída de informações de [Tarefa: programas de software definidos pela organização e/ou aplicativos] para garantir que as informações sejam consistentes com o conteúdo esperado.  
  
**Guia Adicional:**Certos tipos de ataques cibernéticos (por exemplo, injeções de SQL) produzem resultados de saída inesperados ou inconsistentes com os resultados de saída que normalmente seriam esperados de programas ou aplicativos de software. Esse aprimoramento de controle se concentra na detecção de conteúdo estranho, evitando que esse conteúdo estranho seja exibido e alertando as ferramentas de monitoramento de que um comportamento anormal foi descoberto.

## SI-16: Proteção de Memória (P1)

**Descrição do Controle:**O sistema de informações implementa [Atribuição: salvaguardas de segurança definidas pela organização] para proteger sua memória da execução não autorizada de código.  
  
**Guia Adicional:**Alguns adversários iniciam ataques com a intenção de executar código em regiões não executáveis da memória ou em locais de memória proibidos. As salvaguardas de segurança empregadas para proteger a memória incluem, por exemplo, prevenção de execução de dados e randomização do layout do espaço de endereço. As salvaguardas de prevenção de execução de dados podem ser aplicadas por hardware ou por software, fornecendo a maior força do mecanismo.

## SI-17: Procedimentos Seguros (P0)

**Descrição do Controle:**O sistema de informações implementa [Atribuição: procedimentos de segurança definidos pela organização] quando [Atribuição: condições de falha definidas pela organização ocorrem].  
  
**Guia Adicional:**As condições de falha incluem, por exemplo, perda de comunicação entre componentes críticos do sistema ou entre componentes do sistema e instalações operacionais. Os procedimentos à prova de falhas incluem, por exemplo, alertar a equipe do operador e fornecer instruções específicas sobre as etapas subsequentes a serem tomadas (por exemplo, não fazer nada, restabelecer configurações do sistema, encerrar processos, reiniciar o sistema ou entrar em contato com a equipe organizacional designada).

# SA - Aquisição de Sistemas e Serviços

## SA-1: Política e Procedimentos de Aquisição de Sistemas e Serviços (P1)

**Descrição do Controle:**A organização:  
  
a. Desenvolve, documenta e divulga para [Atribuição: pessoal ou funções definidas pela organização]:  
  
1. Uma política de aquisição de sistemas e serviços que aborda finalidade, escopo, funções, responsabilidades, compromisso gerencial, coordenação entre entidades organizacionais e conformidade; e  
  
2. Procedimentos para facilitar a implementação da política de aquisição de sistemas e serviços e controles associados de aquisição de sistemas e serviços; e  
  
b. Analisa e atualiza a atual:  
  
1. Política de aquisição de sistemas e serviços [Atribuição: frequência definida pela organização]; e  
  
2. Procedimentos de aquisição de sistemas e serviços [Atribuição: frequência definida pela organização].  
  
**Guia Adicional:**Esse controle trata do estabelecimento de políticas e procedimentos para a implementação efetiva de controles de segurança selecionados e aprimoramentos de controle na família SA. As políticas e procedimentos refletem as leis federais aplicáveis, ordens executivas, diretivas, regulamentos, políticas, normas e diretrizes. Políticas e procedimentos do programa de segurança no nível da organização podem tornar desnecessária a necessidade de políticas e procedimentos específicos do sistema. A política pode ser incluída como parte da política geral de segurança da informação para organizações ou, inversamente, pode ser representada por múltiplas políticas refletindo a natureza complexa de certas organizações. Os procedimentos podem ser estabelecidos para o programa de segurança em geral e para sistemas de informação específicos, se necessário. A estratégia de gerenciamento de risco organizacional é um fator chave no estabelecimento de políticas e procedimentos.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-12 | https://csrc.nist.gov/publications/search?keywords-lg=800-12 |
| Publicação Especial NIST 800-100 | https://csrc.nist.gov/publications/search?keywords-lg=800-100 |

## SA-2: Alocação de Recursos (P1)

**Descrição do Controle:**A organização:  
  
a. Determina os requisitos de segurança da informação para o sistema de informação ou serviço de sistema de informação no planejamento de processos de missão / negócios;  
  
b. Determina, documenta e aloca os recursos necessários para proteger o sistema de informação ou o serviço de sistema de informação como parte de seu processo de planejamento de capital e controle de investimentos; e  
  
c. Estabelece um item de linha discreto para segurança da informação na documentação organizacional de programação e orçamento.  
  
**Guia Adicional:**A alocação de recursos para segurança da informação inclui financiamento para o sistema inicial de informações ou aquisição de serviços do sistema de informações e financiamento para a manutenção do sistema / serviço.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-65 | https://csrc.nist.gov/publications/search?keywords-lg=800-65 |

## SA-3: Ciclo de Vida de Desenvolvimento do Sistema (P1)

**Descrição do Controle:**A organização:  
  
a. Gerencia o sistema de informações usando [Atribuição: ciclo de vida de desenvolvimento do sistema definido pela organização] que incorpora considerações de segurança da informação;  
  
b. Define e documenta as funções e responsabilidades de segurança da informação ao longo do ciclo de vida de desenvolvimento do sistema;  
  
c. Identifica indivíduos com funções e responsabilidades de segurança da informação; e  
  
d. Integra o processo de gerenciamento de riscos à segurança da informação organizacional nas atividades do ciclo de vida de desenvolvimento do sistema.  
  
**Guia Adicional:**Um ciclo de vida de desenvolvimento de sistema bem definido fornece a base para o desenvolvimento, implementação e operação bem-sucedidos dos sistemas de informações organizacionais. A aplicação dos controles de segurança necessários no ciclo de vida de desenvolvimento do sistema requer um entendimento básico de segurança da informação, ameaças, vulnerabilidades, impactos adversos e riscos a missões críticas / funções de negócios. Os princípios de engenharia de segurança no SA-8 não podem ser aplicados adequadamente se indivíduos que projetam, codificam e testam sistemas de informação e componentes de sistema (incluindo produtos de tecnologia da informação) não entendem a segurança. Portanto, as organizações incluem pessoal qualificado, por exemplo, diretores de segurança da informação, arquitetos de segurança, engenheiros de segurança e oficiais de segurança do sistema de informações nas atividades do ciclo de vida de desenvolvimento do sistema para garantir que os requisitos de segurança sejam incorporados aos sistemas de informações organizacionais. É igualmente importante que os desenvolvedores incluam pessoas na equipe de desenvolvimento que possuam os conhecimentos e habilidades de segurança necessários para garantir que os recursos de segurança necessários sejam efetivamente integrados ao sistema de informações. Os programas de conscientização e treinamento em segurança podem ajudar a garantir que indivíduos com funções e responsabilidades importantes de segurança tenham a experiência, as habilidades e os conhecimentos adequados para conduzir as atividades de ciclo de vida de desenvolvimento do sistema. A integração efetiva dos requisitos de segurança na arquitetura corporativa também ajuda a garantir que considerações importantes sobre segurança sejam abordadas no início do ciclo de vida de desenvolvimento do sistema e que essas considerações estejam diretamente relacionadas à missão organizacional / processos de negócios. Esse processo também facilita a integração da arquitetura de segurança da informação na arquitetura corporativa, consistente com o gerenciamento de riscos organizacionais e as estratégias de segurança da informação.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-37 | https://csrc.nist.gov/publications/search?keywords-lg=800-37 |
| Publicação Especial NIST 800-64 | https://csrc.nist.gov/publications/search?keywords-lg=800-64 |

## SA-4: Processo de Aquisição (P1)

**Descrição do Controle:**A organização inclui os seguintes requisitos, descrições e critérios, explícita ou por referência, no contrato de aquisição do sistema de informações, componente do sistema ou serviço do sistema de informações de acordo com as leis federais aplicáveis, ordens executivas, diretrizes, diretivas, políticas, regulamentos, normas , diretrizes e missão organizacional / necessidades de negócios:  
  
a. Requisitos funcionais de segurança;  
  
b. Requisitos de força de segurança;  
  
c. Requisitos de garantia de segurança;  
  
d. Requisitos de documentação relacionados à segurança;  
  
e. Requisitos para proteger a documentação relacionada à segurança;  
  
f. Descrição do ambiente de desenvolvimento do sistema de informação e do ambiente em que o sistema se destina a operar; e  
  
g. Critérios de aceitação.  
  
**Guia Adicional:**Os componentes do sistema de informação são ativos discretos e identificáveis de tecnologia da informação (por exemplo, hardware, software ou firmware) que representam os componentes de um sistema de informação. Os componentes do sistema de informação incluem produtos comerciais de tecnologia da informação. Os requisitos funcionais de segurança incluem recursos de segurança, funções de segurança e mecanismos de segurança. Os requisitos de força de segurança associados a esses recursos, funções e mecanismos incluem grau de correção, perfeição, resistência ao ataque direto e resistência à violação ou desvio. Os requisitos de garantia de segurança incluem: (i) processos, procedimentos, práticas e metodologias de desenvolvimento; e (ii) evidências de atividades de desenvolvimento e avaliação que fundamentam a confiança de que a funcionalidade de segurança necessária foi implementada e a força de segurança necessária foi alcançada. Os requisitos de documentação de segurança abordam todas as fases do ciclo de vida de desenvolvimento do sistema. Os requisitos de funcionalidade, garantia e documentação de segurança são expressos em termos de controles de segurança e aprimoramentos de controle que foram selecionados através do processo de adaptação. O processo de adaptação do controle de segurança inclui, por exemplo, a especificação de valores de parâmetros por meio do uso de instruções de atribuição e seleção e a especificação de dependências da plataforma e informações de implementação. A documentação de segurança fornece orientação ao usuário e administrador sobre a implementação e operação dos controles de segurança. O nível de detalhe exigido na documentação de segurança baseia-se na categoria de segurança ou no nível de classificação do sistema de informações e no grau em que as organizações dependem da capacidade, funções ou mecanismos de segurança declarados para atender às expectativas gerais de resposta a riscos (conforme definido na organização). estratégia de gerenciamento de riscos). Os requisitos de segurança também podem incluir definições de configuração obrigatórias da organização, especificando funções, portas, protocolos e serviços permitidos. Os critérios de aceitação para sistemas de informação, componentes de sistema de informação e serviços de sistema de informação são definidos da mesma maneira que esses critérios para qualquer aquisição ou aquisição organizacional. A Seção 7.103 do Regulamento Federal de Aquisição (FAR) contém requisitos de segurança da informação do FISMA.  
  
**Melhorias do Controle:**

### SA-4(1): Processo de Aquisição | Propriedades Funcionais dos Controlos de Segurança

A organização exige que o desenvolvedor do sistema de informações, componente do sistema ou serviço do sistema de informações forneça uma descrição das propriedades funcionais dos controles de segurança a serem empregados.  
Guia Adicional: As propriedades funcionais dos controles de segurança descrevem a funcionalidade (ou seja, capacidade, funções ou mecanismos de segurança) visível nas interfaces dos controles e excluem especificamente a funcionalidade e as estruturas de dados internas à operação dos controles.

### SA-4(2): Processo de Aquisição | Informação de Projeto/Implementação para Controlos de Segurança

A organização exige que o desenvolvedor do sistema de informações, componente do sistema ou serviço do sistema de informações forneça informações de design e implementação dos controles de segurança a serem empregados, incluindo: [Seleção (uma ou mais): interfaces de sistema externas relevantes à segurança; design de alto nível; design de baixo nível; código fonte ou esquemas de hardware; [Atribuição: informações de projeto / implementação definidas pela organização]] em [Atribuição: nível de detalhe definido pela organização].  
Guia Adicional: As organizações podem exigir diferentes níveis de detalhe na documentação de design e implementação dos controles de segurança empregados em sistemas de informações organizacionais, componentes de sistema ou serviços de sistemas de informação com base em requisitos de missão / negócios, requisitos de confiabilidade / resiliência e requisitos de análise e teste. Os sistemas de informação podem ser particionados em vários subsistemas. Cada subsistema dentro do sistema pode conter um ou mais módulos. O design de alto nível do sistema é expresso em termos de vários subsistemas e nas interfaces entre os subsistemas, fornecendo funcionalidade relevante à segurança. O design de baixo nível do sistema é expresso em termos de módulos, com ênfase especial no software e firmware (mas não excluindo o hardware) e nas interfaces entre os módulos, oferecendo funcionalidade relevante à segurança. O código-fonte e os esquemas de hardware são geralmente referidos como a representação de implementação do sistema de informações.

### SA-4(3): Processo de Aquisição | Métodos / Técnicas / Práticas de Desenvolvimento

A organização exige que o desenvolvedor do sistema de informações, componente do sistema ou serviço do sistema de informações demonstre o uso de um ciclo de vida de desenvolvimento do sistema que inclui [Atribuição: métodos de engenharia de segurança / sistema de práticas definidas pela organização, desenvolvimento de software métodos, técnicas de teste / avaliação / validação e processos de controle de qualidade].  
Guia Adicional: Seguir um ciclo de vida de desenvolvimento de sistema bem definido que inclui métodos de desenvolvimento de software de última geração, métodos de engenharia de sistemas / segurança, processos de controle de qualidade e técnicas de teste, avaliação e validação ajuda a reduzir o número e a gravidade dos erros latentes dentro de sistemas de informação, componentes de sistema e serviços de sistema de informação. Reduzir o número / gravidade de tais erros reduz o número de vulnerabilidades nesses sistemas, componentes e serviços.

### SA-4(4): Processo de Aquisição | Atribuição de Componentes a Sistemas

[Retirado: Incorporado ao CM-8 (9)].

### SA-4(5): Processo de Aquisição | Configurações do Sistema / Componente / Serviço

A organização exige que o desenvolvedor do sistema de informações, componente do sistema ou serviço do sistema de informações:  
  
a. Entregue o sistema, componente ou serviço com [Atribuição: configurações de segurança definidas pela organização] implementadas; e  
  
b. Use as configurações como padrão para qualquer reinstalação ou atualização subsequente do sistema, componente ou serviço.  
Guia Adicional: As configurações de segurança incluem, por exemplo, a linha de base de configuração do governo dos EUA (USGCB) e quaisquer limitações de funções, portas, protocolos e serviços. As características de segurança incluem, por exemplo, exigir que todas as senhas padrão tenham sido alteradas.

### SA-4(6): Processo de Aquisição | Uso de Produtos de Garantia da Informação

A organização:  
  
a. Emprega apenas produtos governamentais prontos para uso comercial (GOTS) ou comercialmente garantidos (IA), garantia de informação (IA) e produtos de tecnologia da informação habilitados para IA que compõem uma solução aprovada pela NSA para proteger as informações classificadas quando as redes usadas para transmitir as informações estão em um nível de classificação inferior ao das informações transmitidas; e  
  
b. Garante que esses produtos tenham sido avaliados e/ou validados pela NSA ou de acordo com os procedimentos aprovados pela NSA.  
Guia Adicional: Os produtos de tecnologia da informação habilitados para COTS IA ou IA usados para proteger informações classificadas por meios criptográficos podem ser necessários para usar o gerenciamento de chaves aprovado pela NSA.

### SA-4(7): Processo de Aquisição | Perfis de Proteção Aprovados para NIAP

A organização:  
  
a. Limita o uso de produtos de garantia da informação (IA) fornecidos comercialmente e de tecnologia da informação habilitados para IA aos produtos que foram avaliados com sucesso em relação a um Perfil de proteção aprovado pela parceria com a National Information Assurance (NIAP) para um tipo de tecnologia específico, se esse perfil existir ; e  
  
b. Requer, se não existir um Perfil de proteção aprovado pelo NIAP para um tipo de tecnologia específico, mas um produto de tecnologia da informação fornecido comercialmente confiar na funcionalidade criptográfica para impor sua política de segurança, que o módulo criptográfico seja validado por FIPS.

### SA-4(8): Processo de Aquisição | Plano de Monitoramento Contínuo

A organização exige que o desenvolvedor do sistema de informações, componente do sistema ou serviço do sistema de informações produza um plano para o monitoramento contínuo da eficácia do controle de segurança que contém [Atribuição: nível de detalhe definido pela organização].  
Guia Adicional: O objetivo dos planos de monitoramento contínuo é determinar se o conjunto completo de controles de segurança planejados, necessários e implantados no sistema de informações, componente do sistema ou serviço do sistema de informações continua a ser eficaz ao longo do tempo com base nas mudanças inevitáveis que ocorrem. Os planos de monitoramento contínuo do desenvolvedor incluem um nível de detalhe suficiente para que as informações possam ser incorporadas às estratégias e programas de monitoramento contínuo implementados pelas organizações.

### SA-4(9): Processo de Aquisição | Funções / Portos / Protocolos / Serviços em Uso

A organização exige que o desenvolvedor do sistema de informações, componente do sistema ou serviço do sistema de informações identifique, no início do ciclo de vida do desenvolvimento do sistema, as funções, portas, protocolos e serviços destinados ao uso organizacional.  
Guia Adicional: A identificação de funções, portas, protocolos e serviços no início do ciclo de vida de desenvolvimento do sistema (por exemplo, durante as fases iniciais de definição e design de requisitos) permite que as organizações influenciem o design do sistema de informação, componente do sistema de informação ou serviço do sistema de informação. Esse envolvimento precoce no ciclo de vida ajuda as organizações a evitar ou minimizar o uso de funções, portas, protocolos ou serviços que apresentam riscos desnecessariamente altos e a entender as vantagens e desvantagens envolvidas no bloqueio de portas, protocolos ou serviços específicos (ou ao exigir informações prestadores de serviços do sistema). A identificação antecipada de funções, portas, protocolos e serviços evita a atualização onerosa dos controles de segurança após a implementação do sistema de informações, componente do sistema ou serviço do sistema de informações. O SA-9 descreve os requisitos para serviços de sistema de informações externas com organizações que identificam quais funções, portas, protocolos e serviços são fornecidos a partir de fontes externas.

### SA-4(10): Processo de Aquisição | Uso de Produtos PIV Aprovados

A organização emprega apenas produtos de tecnologia da informação na lista de produtos aprovados pelo FIPS 201 para recursos de Verificação de identidade pessoal (PIV) implementados nos sistemas de informações organizacionais.

**Referências:**

|  |  |
| --- | --- |
| DHS - HSPD-12 | https://www.dhs.gov/homeland-security-presidential-directive-12 |
| ISO 15408 | http://www.iso.org/iso/iso\_catalogue/catalogue\_tc/catalogue\_detail.htm?csnumber=50341 |
| Publicações de Normas Federais de Processamento de Informações N.201 | http://csrc.nist.gov/publications/PubsFIPS.html#201 |
| Publicação Especial NIST 800-23 | https://csrc.nist.gov/publications/search?keywords-lg=800-23 |
| Publicação Especial NIST 800-35 | https://csrc.nist.gov/publications/search?keywords-lg=800-35 |
| Publicação Especial NIST 800-36 | https://csrc.nist.gov/publications/search?keywords-lg=800-36 |
| Publicação Especial NIST 800-37 | https://csrc.nist.gov/publications/search?keywords-lg=800-37 |
| Publicação Especial NIST 800-64 | https://csrc.nist.gov/publications/search?keywords-lg=800-64 |
| Publicação Especial NIST 800-70 | https://csrc.nist.gov/publications/search?keywords-lg=800-70 |
| Publicação Especial NIST 800-137 | https://csrc.nist.gov/publications/search?keywords-lg=800-137 |
| Regulamento de Aquisição Federal | https://acquisition.gov/far |
| NIAP: Parceria Nacional de Garantia da Informação | http://www.niap-ccevs.org |

## SA-5: Documentação do Sistema de Informação (P2)

**Descrição do Controle:**A organização:  
  
a. Obtém documentação do administrador para o sistema de informações, componente do sistema ou serviço do sistema de informações que descreve:  
  
1. Configuração, instalação e operação seguras do sistema, componente ou serviço;  
  
2. Uso e manutenção eficazes de funções / mecanismos de segurança; e  
  
3. Vulnerabilidades conhecidas relacionadas à configuração e uso de funções administrativas (ou seja, privilegiadas);  
  
b. Obtém a documentação do usuário para o sistema de informações, componente do sistema ou serviço do sistema de informações que descreve:  
  
1. Funções / mecanismos de segurança acessíveis ao usuário e como usar efetivamente essas funções / mecanismos de segurança;  
  
2. Métodos de interação do usuário, que permitem que os indivíduos usem o sistema, componente ou serviço de maneira mais segura; e  
  
3. Responsabilidades do usuário em manter a segurança do sistema, componente ou serviço;  
  
c. O Documents tenta obter a documentação do sistema de informações, componente do sistema ou serviço do sistema de informações quando essa documentação está indisponível ou inexistente e recebe [Atribuição: ações definidas pela organização] em resposta;  
  
d. Protege a documentação conforme necessário, de acordo com a estratégia de gerenciamento de riscos; e  
  
e. Distribui a documentação para [Atribuição: pessoal ou funções definidas pela organização].  
  
**Guia Adicional:**Esse controle ajuda a equipe organizacional a entender a implementação e operação dos controles de segurança associados aos sistemas de informação, componentes do sistema e serviços do sistema de informação. As organizações consideram o estabelecimento de medidas específicas para determinar a qualidade / integridade do conteúdo fornecido. A incapacidade de obter a documentação necessária pode ocorrer, por exemplo, devido à idade do sistema / componente de informação ou à falta de suporte de desenvolvedores e contratados. Nessas situações, as organizações podem precisar recriar a documentação selecionada se essa documentação for essencial para a implementação ou operação efetiva dos controles de segurança. O nível de proteção fornecido para o sistema de informações, componente ou documentação de serviço selecionada é proporcional à categoria ou classificação de segurança do sistema. Por exemplo, a documentação associada a um sistema chave de armas do DoD ou a um sistema de comando e controle normalmente exigiria um nível de proteção mais alto do que um sistema administrativo de rotina. A documentação que trata das vulnerabilidades do sistema de informações também pode exigir um nível maior de proteção. A operação segura do sistema de informações inclui, por exemplo, o início inicial do sistema e a retomada da operação segura do sistema após qualquer lapso na operação do sistema.  
  
**Melhorias do Controle:**

### SA-5(1): Documentação do Sistema de Informação | Propriedades Funcionais dos Controlos de Segurança

[Retirado: Incorporado na SA-4 (1)].

### SA-5(2): Documentação do Sistema de Informação | Interfaces do Sistema Externo Relevantes da Segurança

[Retirado: Incorporado na SA-4 (2)].

### SA-5(3): Documentação do Sistema de Informação | Design de Alto Nível

[Retirado: Incorporado na SA-4 (2)].

### SA-5(4): Documentação do Sistema de Informação | Projeto de Baixo Nível

[Retirado: Incorporado na SA-4 (2)].

### SA-5(5): Documentação do Sistema de Informação | Código Fonte

[Retirado: Incorporado na SA-4 (2)].

## SA-6: Restrições de Uso de Software (P0)

**Descrição do Controle:**[Retirado: incorporado no CM-10 e SI-7].

## SA-7: Software Instalado pelo Usuário (P0)

**Descrição do Controle:**[Retirado: Incorporado no CM-11 e SI-7].

## SA-8: Princípios da Engenharia de Segurança (P1)

**Descrição do Controle:**A organização aplica os princípios de engenharia de segurança do sistema de informação na especificação, design, desenvolvimento, implementação e modificação do sistema de informação.  
  
**Guia Adicional:**As organizações aplicam os princípios de engenharia de segurança principalmente a novos sistemas ou sistemas de informações de desenvolvimento submetidos a grandes atualizações. Para sistemas legados, as organizações aplicam os princípios de engenharia de segurança às atualizações e modificações do sistema, na medida do possível, dado o estado atual de hardware, software e firmware nesses sistemas. Os princípios de engenharia de segurança incluem, por exemplo: (i) desenvolvimento de proteções em camadas; (ii) estabelecer políticas, arquitetura e controles de segurança sólidos como base para o design; (iii) incorporar requisitos de segurança no ciclo de vida de desenvolvimento do sistema; (iv) delinear limites físicos e lógicos de segurança; (v) garantir que os desenvolvedores do sistema sejam treinados sobre como criar software seguro; (vi) adequar os controles de segurança para atender às necessidades organizacionais e operacionais; (vii) executar modelagem de ameaças para identificar casos de uso, agentes de ameaças, vetores de ataque e padrões de ataque, além de compensar controles e padrões de design necessários para mitigar os riscos; e (viii) reduzir o risco a níveis aceitáveis, possibilitando decisões informadas sobre o gerenciamento de riscos.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-27 | https://csrc.nist.gov/publications/search?keywords-lg=800-27 |

## SA-9: Serviços Externos do Sistema de Informação (P1)

**Descrição do Controle:**A organização:  
  
a. Requer que os provedores de serviços externos de sistemas de informações cumpram os requisitos de segurança das informações organizacionais e usem [Atribuição: controles de segurança definidos pela organização] de acordo com as leis federais aplicáveis, Ordens Executivas, Ordens Executivas, diretivas, diretivas, políticas, regulamentos, normas e orientações;  
  
b. Define e documenta a supervisão governamental e as funções e responsabilidades dos usuários em relação aos serviços externos de sistemas de informação; e  
  
c. Emprega [Atribuição: processos, métodos e técnicas definidos pela organização] para monitorar continuamente a conformidade do controle de segurança por provedores de serviços externos.  
  
**Guia Adicional:**Serviços de sistema de informações externas são serviços implementados fora dos limites de autorização dos sistemas de informações organizacionais. Isso inclui serviços que são usados por, mas não fazem parte de sistemas de informações organizacionais. A política do FISMA e OMB exige que as organizações que usam provedores de serviços externos que estão processando, armazenando ou transmitindo informações federais ou sistemas de informações operacionais em nome do governo federal garantam que esses provedores atendam aos mesmos requisitos de segurança que os órgãos federais devem cumprir. As organizações estabelecem relacionamentos com prestadores de serviços externos de várias maneiras, incluindo, por exemplo, joint ventures, parcerias comerciais, contratos, acordos interinstitucionais, acordos de linhas de negócios, acordos de licenciamento e trocas na cadeia de suprimentos. A responsabilidade pelo gerenciamento de riscos do uso de serviços externos de sistemas de informações permanece com as autoridades autorizadoras. Para serviços externos às organizações, uma cadeia de confiança exige que as organizações estabeleçam e mantenham um nível de confiança de que cada provedor participante no relacionamento potencialmente complexo consumidor-provedor forneça proteção adequada aos serviços prestados. A extensão e a natureza dessa cadeia de confiança variam de acordo com o relacionamento entre as organizações e os fornecedores externos. As organizações documentam a base dos relacionamentos de confiança para que os relacionamentos possam ser monitorados ao longo do tempo. A documentação de serviços do sistema de informações externas inclui governo, provedores de serviços, funções e responsabilidades de segurança do usuário final e acordos de nível de serviço. Os contratos de nível de serviço definem as expectativas de desempenho dos controles de segurança, descrevem resultados mensuráveis e identificam soluções e requisitos de resposta para instâncias identificadas de não conformidade.  
  
**Melhorias do Controle:**

### SA-9(1): Serviços Externos do Sistema de Informação | Avaliações de Riscos / Aprovações Organizacionais

A organização:  
  
a. Realiza uma avaliação organizacional dos riscos antes da aquisição ou terceirização de serviços dedicados de segurança da informação; e  
  
b. Garante que a aquisição ou terceirização de serviços dedicados de segurança da informação seja aprovada por [Designação: pessoal ou funções definidas pela organização].  
Guia Adicional: Os serviços dedicados de segurança da informação incluem, por exemplo, monitoramento, análise e resposta a incidentes, operação de dispositivos relacionados à segurança da informação, como firewalls ou serviços de gerenciamento de chaves.

### SA-9(2): Serviços Externos do Sistema de Informação | Identificação de Funções / Portos / Protocolos / Serviços

A organização exige que os fornecedores de [Designação: serviços de sistema de informação externo definidos pela organização] identifiquem as funções, portas, protocolos e outros serviços necessários para o uso de tais serviços.  
Guia Adicional: As informações de provedores de serviços externos sobre as funções, portas, protocolos e serviços específicos usados na prestação desses serviços podem ser particularmente úteis quando houver necessidade de entender as compensações envolvidas na restrição de determinadas funções / serviços ou no bloqueio de determinadas portas / protocolos .

### SA-9(3): Serviços Externos do Sistema de Informação | Estabelecer / Manter O Relacionamento de Confiança com os Fornecedores

A organização estabelece, documenta e mantém relacionamentos de confiança com provedores de serviços externos com base em [Atribuição: requisitos, propriedades, fatores ou condições de segurança definidos pela organização que definem relacionamentos de confiança aceitáveis].  
Guia Adicional: O grau de confiança de que o risco de usar serviços externos está em um nível aceitável depende da confiança que as organizações depositam nos fornecedores externos, individualmente ou em conjunto. Os relacionamentos de confiança podem ajudar a organização a obter níveis crescentes de confiança de que os provedores de serviços participantes estão fornecendo proteção adequada para os serviços prestados. Esses relacionamentos podem ser complicados devido ao número de entidades em potencial que participam das interações consumidor-fornecedor, relacionamentos subordinados e níveis de confiança e os tipos de interações entre as partes. Em alguns casos, o grau de confiança se baseia na quantidade de organizações de controle direto capazes de exercer em prestadores de serviços externos no que diz respeito ao emprego de controles de segurança necessários para a proteção do serviço / informação e as evidências apresentadas quanto à eficácia desses controles. O nível de controle é normalmente estabelecido pelos termos e condições dos contratos ou acordos de nível de serviço e pode variar de controle extensivo (por exemplo, contratos de negociação ou acordos que especificam requisitos de segurança para os provedores) a controle muito limitado (por exemplo, uso de contratos ou acordos de nível de serviço para obter serviços de commodities, como serviços de telecomunicações comerciais). Em outros casos, os níveis de confiança são baseados em fatores que convencem as organizações que exigiram controles de segurança e que existem determinações de eficácia do controle. Por exemplo, serviços de sistemas de informações externos autorizados separadamente, fornecidos às organizações por meio de relacionamentos comerciais bem estabelecidos, podem fornecer graus de confiança em tais serviços dentro da faixa de risco tolerável das organizações que usam os serviços. Os provedores de serviços externos também podem terceirizar os serviços selecionados para outras entidades externas, tornando a relação de confiança mais difícil e complicada de gerenciar. Dependendo da natureza dos serviços, as organizações podem achar muito difícil confiar significativamente em fornecedores externos. Isso não se deve a qualquer falta de confiança inerente por parte dos provedores, mas ao nível intrínseco de risco nos serviços.

### SA-9(4): Serviços Externos do Sistema de Informação | Interesses Consistentes de Consumidores e Prestadores

A organização emprega [Atribuição: salvaguardas de segurança definidas pela organização] para garantir que os interesses dos [Atribuição: provedores de serviços externos definidos pela organização] sejam consistentes e reflitam os interesses da organização.  
Guia Adicional: À medida que as organizações usam cada vez mais provedores de serviços externos, existe a possibilidade de que os interesses dos provedores de serviços possam divergir dos interesses da organização. Em tais situações, simplesmente ter as salvaguardas técnicas, processuais ou operacionais corretas em vigor pode não ser suficiente se os prestadores de serviços que implementam e controlam essas salvaguardas não estiverem operando de maneira consistente com os interesses das organizações consumidoras. As possíveis ações que as organizações podem adotar para lidar com essas preocupações incluem, por exemplo, exigir verificações de antecedentes para a equipe selecionada de prestadores de serviços, examinar registros de propriedade, empregar apenas prestadores de serviços confiáveis (ou seja, fornecedores com os quais as organizações tiveram experiências positivas) e realizar / visitas não programadas às instalações do provedor de serviços.

### SA-9(5): Serviços Externos do Sistema de Informação | Local de Processamento, Armazenamento e Serviço

A organização restringe a localização de [Seleção (uma ou mais): processamento de informações; informação / dados; serviços do sistema de informações] para [Atribuição: locais definidos pela organização] com base em [Atribuição: requisitos ou condições definidos pela organização].  
Guia Adicional: A localização do processamento de informações, armazenamento de informações / dados ou serviços do sistema de informações críticos para as organizações pode ter um impacto direto na capacidade dessas organizações de executar com êxito suas missões / funções de negócios. Esta situação existe quando fornecedores externos controlam a localização do processamento, armazenamento ou serviços. Os critérios que os fornecedores externos usam para a seleção de locais de processamento, armazenamento ou serviço podem ser diferentes dos critérios organizacionais. Por exemplo, as organizações podem querer garantir que os locais de armazenamento de dados / informações sejam restritos a determinados locais para facilitar as atividades de resposta a incidentes (por exemplo, análises forenses, investigações posteriores) em caso de violações / comprometimentos da segurança da informação. Tais atividades de resposta a incidentes podem ser afetadas adversamente pelas leis ou protocolos vigentes nos locais onde ocorrem o processamento e o armazenamento e/ou nos locais dos quais emanam os serviços do sistema de informações.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-35 | https://csrc.nist.gov/publications/search?keywords-lg=800-35 |

## SA-10: Gestão da Configuração do Desenvolvedor (P1)

**Descrição do Controle:**A organização exige que o desenvolvedor do sistema de informações, componente do sistema ou serviço do sistema de informações:  
  
a. Executar gerenciamento de configuração durante sistema, componente ou serviço [Seleção (um ou mais): design; desenvolvimento; implementação; Operação];  
  
b. Documentar, gerenciar e controlar a integridade das alterações em [Atribuição: itens de configuração definidos pela organização sob gerenciamento de configuração];  
  
c. Implemente apenas alterações aprovadas pela organização no sistema, componente ou serviço;  
  
d. Documente as alterações aprovadas no sistema, componente ou serviço e os possíveis impactos de segurança dessas alterações; e  
  
e. Rastreie falhas de segurança e resolução de falhas no sistema, componente ou serviço e relate as descobertas para [Designação: pessoal definido pela organização].  
  
**Guia Adicional:**Esse controle também se aplica a organizações que conduzem o desenvolvimento e integração de sistemas de informação internos. As organizações consideram a qualidade e a integridade das atividades de gerenciamento de configuração conduzidas pelos desenvolvedores como evidência da aplicação de salvaguardas de segurança eficazes. As proteções incluem, por exemplo, proteger contra modificação ou destruição não autorizada, as cópias principais de todo o material usado para gerar partes relevantes para a segurança do hardware, software e firmware do sistema. Manter a integridade das alterações no sistema de informações, no componente do sistema de informações ou no sistema de informações requer controle de configuração durante todo o ciclo de vida de desenvolvimento do sistema para rastrear alterações autorizadas e evitar alterações não autorizadas. Os itens de configuração que são colocados sob o gerenciamento de configuração (se a existência / uso for exigido por outros controles de segurança) incluem: o modelo formal; as especificações funcionais, de alto e baixo nível de design; outros dados de projeto; documentação de implementação; código fonte e esquemas de hardware; a versão em execução do código do objeto; ferramentas para comparar novas versões de descrições de hardware relevantes para segurança e código-fonte de software / firmware com versões anteriores; e acessórios de teste e documentação. Dependendo das necessidades de missão / negócios das organizações e da natureza das relações contratuais estabelecidas, os desenvolvedores podem fornecer suporte ao gerenciamento de configuração durante as fases de operação e manutenção do ciclo de vida.  
  
**Melhorias do Controle:**

### SA-10(1): Gestão da Configuração do Desenvolvedor | Verificação de Integridade de Software / Firmware

A organização exige que o desenvolvedor do sistema de informações, componente do sistema ou serviço do sistema de informações permita a verificação da integridade dos componentes de software e firmware.  
Guia Adicional: Esse aprimoramento de controle permite que as organizações detectem alterações não autorizadas nos componentes de software e firmware através do uso de ferramentas, técnicas e/ou mecanismos fornecidos pelos desenvolvedores. Os mecanismos de verificação de integridade também podem lidar com a falsificação de componentes de software e firmware. As organizações verificam a integridade dos componentes de software e firmware, por exemplo, através de hashes unidirecionais seguros fornecidos pelos desenvolvedores. Os componentes de software e firmware fornecidos também incluem quaisquer atualizações para esses componentes.

### SA-10(2): Gestão da Configuração do Desenvolvedor | Processos Alternativos de Gerenciamento de Configuração

A organização fornece um processo de gerenciamento de configuração alternativo usando o pessoal da organização na ausência de uma equipe de gerenciamento de configuração de desenvolvedor dedicada.  
Guia Adicional: Processos alternativos de gerenciamento de configuração podem ser necessários, por exemplo, quando as organizações usam produtos comerciais de tecnologia da informação disponíveis no mercado (COTS). Os processos de gerenciamento de configuração alternativa incluem pessoal organizacional que: (i) é responsável por revisar / aprovar as alterações propostas nos sistemas de informação, componentes do sistema e serviços do sistema de informação; e (ii) realizar análises de impacto na segurança antes da implementação de quaisquer alterações nos sistemas, componentes ou serviços (por exemplo, uma placa de controle de configuração que considere os impactos na segurança das mudanças durante o desenvolvimento e inclua representantes da organização e do desenvolvedor, quando aplicável )

### SA-10(3): Gestão da Configuração do Desenvolvedor | Verificação de Integridade de Hardware

A organização requer que o desenvolvedor do sistema de informações, componente do sistema ou serviço do sistema de informações permita a verificação da integridade dos componentes de hardware.  
Guia Adicional: Esse aprimoramento de controle permite que as organizações detectem alterações não autorizadas nos componentes de hardware através do uso de ferramentas, técnicas e/ou mecanismos fornecidos pelos desenvolvedores. As organizações verificam a integridade dos componentes de hardware, por exemplo, com etiquetas de difícil cópia e números de série verificáveis fornecidos pelos desenvolvedores e exigindo a implementação de tecnologias anti-adulteração. Os componentes de hardware fornecidos também incluem atualizações para esses componentes.

### SA-10(4): Gestão da Configuração do Desenvolvedor | Geração Confiável

A organização exige que o desenvolvedor do sistema de informações, componente do sistema ou serviço do sistema de informações empregue ferramentas para comparar versões recém-geradas de descrições de hardware relevantes à segurança e código-fonte e objeto de software / firmware com versões anteriores.  
Guia Adicional: Esse aprimoramento de controle aborda alterações nos componentes de hardware, software e firmware entre as versões durante o desenvolvimento. Por outro lado, o SA-10 (1) e o SA-10 (3) permitem que as organizações detectem alterações não autorizadas nos componentes de hardware, software e firmware por meio do uso de ferramentas, técnicas e/ou mecanismos fornecidos pelos desenvolvedores.

### SA-10(5): Gestão da Configuração do Desenvolvedor | Integridade de Mapeamento para Controle de Versões

A organização exige que o desenvolvedor do sistema de informações, componente do sistema ou serviço do sistema de informações mantenha a integridade do mapeamento entre os dados principais da construção (desenhos de hardware e código de software / firmware) que descrevem a versão atual de hardware, software relevante para segurança, e firmware e a cópia mestre no local dos dados para a versão atual.  
Guia Adicional: Esse aprimoramento de controle aborda alterações nos componentes de hardware, software e firmware durante o desenvolvimento inicial e durante as atualizações do ciclo de vida do sistema. Manter a integridade entre as cópias mestras de hardware, software e firmware relevantes à segurança (incluindo designs e código-fonte) e os dados equivalentes nas cópias mestres no local em ambientes operacionais é essencial para garantir a disponibilidade de sistemas de informações organizacionais que suportam missões críticas e/ou funções comerciais.

### SA-10(6): Gestão da Configuração do Desenvolvedor | Distribuição Confiável

A organização exige que o desenvolvedor do sistema de informações, componente do sistema ou serviço do sistema de informações execute procedimentos para garantir que as atualizações de hardware, software e firmware relevantes à segurança distribuídas à organização sejam exatamente as especificadas nas cópias mestras.  
Guia Adicional: A distribuição confiável de atualizações de hardware, software e firmware relevantes para a segurança ajuda a garantir que essas atualizações sejam representações fiéis das cópias principais mantidas pelo desenvolvedor e que não foram violadas durante a distribuição.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-128 | https://csrc.nist.gov/publications/search?keywords-lg=800-128 |

## SA-11: Teste e Avaliação da Segurança do Desenvolvedor (P1)

**Descrição do Controle:**A organização exige que o desenvolvedor do sistema de informações, componente do sistema ou serviço do sistema de informações:  
  
a. Criar e implementar um plano de avaliação de segurança;  
  
b. Execute [Seleção (um ou mais): unidade; integração; sistema; regressão] teste / avaliação em [Tarefa: profundidade e cobertura definidas pela organização];  
  
c. Produzir evidências da execução do plano de avaliação de segurança e dos resultados dos testes / avaliações de segurança;  
  
d. Implementar um processo de correção de falhas verificável; e  
  
e. Falhas corretas identificadas durante o teste / avaliação de segurança.  
  
**Guia Adicional:**O teste / avaliação de segurança no desenvolvimento ocorre em todas as fases pós-design do ciclo de vida de desenvolvimento do sistema. Esses testes / avaliações confirmam que os controles de segurança necessários foram implementados corretamente, operando conforme o planejado, aplicando a política de segurança desejada e atendendo aos requisitos de segurança estabelecidos. As propriedades de segurança dos sistemas de informação podem ser afetadas pela interconexão dos componentes do sistema ou alterações nesses componentes. Essas interconexões ou alterações (por exemplo, atualização ou substituição de aplicativos e sistemas operacionais) podem afetar adversamente os controles de segurança implementados anteriormente. Esse controle fornece tipos adicionais de teste / avaliação de segurança que os desenvolvedores podem realizar para reduzir ou eliminar possíveis falhas. O teste de aplicativos de software personalizados pode exigir abordagens como análise estática, análise dinâmica, análise binária ou um híbrido das três abordagens. Os desenvolvedores podem empregar essas abordagens de análise em uma variedade de ferramentas (por exemplo, scanners de aplicativos baseados na Web, ferramentas de análise estática, analisadores binários) e em revisões de código-fonte. Os planos de avaliação de segurança fornecem as atividades específicas que os desenvolvedores planejam realizar, incluindo os tipos de análises, testes, avaliação e revisões dos componentes de software e firmware, o grau de rigor a ser aplicado e os tipos de artefatos produzidos durante esses processos. A profundidade dos testes / avaliações de segurança refere-se ao rigor e ao nível de detalhes associados ao processo de avaliação (por exemplo, teste de caixa preta, caixa cinza ou caixa branca). A cobertura do teste / avaliação de segurança refere-se ao escopo (isto é, número e tipo) dos artefatos incluídos no processo de avaliação. Os contratos especificam os critérios de aceitação para planos de avaliação de segurança, processos de correção de falhas e a evidência de que os planos / processos foram aplicados diligentemente. Os métodos para revisar e proteger os planos, evidências e documentação de avaliação são proporcionais à categoria de segurança ou ao nível de classificação do sistema de informação. Os contratos podem especificar requisitos de proteção da documentação.  
  
**Melhorias do Controle:**

### SA-11(1): Teste e Avaliação da Segurança do Desenvolvedor | Análise do Código Estático

A organização exige que o desenvolvedor do sistema de informações, componente do sistema ou serviço do sistema de informações empregue ferramentas estáticas de análise de código para identificar falhas comuns e documentar os resultados da análise.  
Guia Adicional: A análise de código estático fornece uma tecnologia e metodologia para análises de segurança. Essa análise pode ser usada para identificar vulnerabilidades de segurança e impor práticas de codificação de segurança. A análise de código estático é mais eficaz quando usada no início do processo de desenvolvimento, quando cada alteração de código pode ser verificada automaticamente quanto a possíveis pontos fracos. A análise estática pode fornecer orientações claras sobre a correção, além de defeitos, para permitir que os desenvolvedores corrijam esses defeitos. As evidências da implementação correta da análise estática podem incluir, por exemplo, densidade agregada de defeitos para tipos críticos, evidências de que os defeitos foram inspecionados por desenvolvedores ou profissionais de segurança e evidências de que os defeitos foram corrigidos. Uma densidade excessivamente alta de achados ignorados (geralmente chamados de ignorados ou falsos positivos) indica um problema em potencial com o processo ou a ferramenta de análise. Nesses casos, as organizações avaliam a validade das evidências contra evidências de outras fontes.

### SA-11(2): Teste e Avaliação da Segurança do Desenvolvedor | Análises de Ameaças e Vulnerabilidade

A organização exige que o desenvolvedor do sistema de informações, componente do sistema ou serviço do sistema de informações realize análises de ameaças e vulnerabilidades e teste / avaliação subsequente do sistema, componente ou serviço construído.  
Guia Adicional: Os aplicativos podem divergir significativamente das especificações funcionais e de design criadas durante as fases de requisitos e design do ciclo de vida de desenvolvimento do sistema. Portanto, as análises de ameaças e vulnerabilidades dos sistemas de informação, componentes do sistema e serviços do sistema de informação antes da entrega são críticas para a operação eficaz desses sistemas, componentes e serviços. As análises de ameaças e vulnerabilidades nesta fase do ciclo de vida ajudam a garantir que as alterações no projeto ou na implementação tenham sido contabilizadas e que quaisquer novas vulnerabilidades criadas como resultado dessas alterações tenham sido revisadas e mitigadas.

### SA-11(3): Teste e Avaliação da Segurança do Desenvolvedor | Verificação Independente de Planos de Avaliação/Evidência

A organização:  
  
a. Requer um agente independente que atenda a [Atribuição: critérios de independência definidos pela organização] para verificar a implementação correta do plano de avaliação de segurança do desenvolvedor e as evidências produzidas durante o teste / avaliação de segurança; e  
  
b. Garante que o agente independente receba informações suficientes para concluir o processo de verificação ou tenha a autoridade para obtê-las.  
Guia Adicional: Agentes independentes têm as qualificações necessárias (ou seja, conhecimentos, habilidades, treinamento e experiência) para verificar a implementação correta dos planos de avaliação de segurança do desenvolvedor.

### SA-11(4): Teste e Avaliação da Segurança do Desenvolvedor | Revisões de Código Manual

A organização exige que o desenvolvedor do sistema de informações, componente do sistema ou serviço do sistema de informações realize uma revisão manual do código de [Atribuição: código específico definido pela organização] usando [Atribuição: processos, procedimentos e/ou técnicas definidos pela organização].  
Guia Adicional: As revisões manuais de código geralmente são reservadas para os componentes críticos de software e firmware dos sistemas de informação. Essas revisões de código são exclusivamente eficazes na identificação de pontos fracos que exigem conhecimento dos requisitos ou do contexto do aplicativo que geralmente não estão disponíveis para ferramentas e técnicas analíticas mais automatizadas, como análise estática ou dinâmica. Os componentes que se beneficiam da revisão manual incluem, por exemplo, verificar matrizes de controle de acesso em relação aos controles de aplicativos e revisar aspectos mais detalhados de implementações e controles criptográficos.

### SA-11(5): Teste e Avaliação da Segurança do Desenvolvedor | PenTest

A organização exige que o desenvolvedor do sistema de informações, componente do sistema ou serviço do sistema de informações realize testes de penetração em [Atribuição: largura / profundidade definida pela organização] e com [Atribuição: restrições definidas pela organização].  
Guia Adicional: O teste de penetração é uma metodologia de avaliação na qual os avaliadores, usando todos os produtos de tecnologia da informação disponíveis e/ou a documentação do sistema de informações (por exemplo, especificações de design de produto / sistema, código fonte e manuais do administrador / operador) e trabalhando sob restrições específicas, tentam burlar as normas implementadas recursos de segurança de produtos e sistemas de tecnologia da informação. Os testes de penetração podem incluir, por exemplo, testes de caixa branca, cinza ou preta com análises realizadas por profissionais de segurança qualificados, simulando ações adversas. O objetivo do teste de penetração é descobrir possíveis vulnerabilidades em produtos e sistemas de tecnologia da informação resultantes de erros de implementação, falhas de configuração ou outras deficiências ou deficiências na implantação operacional. Os testes de penetração podem ser realizados em conjunto com revisões de código manuais e automatizadas para fornecer níveis mais altos de análise do que normalmente seria possível.

### SA-11(6): Teste e Avaliação da Segurança do Desenvolvedor | Revisões de Superfície de Ataque

A organização exige que o desenvolvedor do sistema de informações, componente do sistema ou serviço do sistema de informações realize análises da superfície de ataque.  
Guia Adicional: As superfícies de ataque dos sistemas de informação são áreas expostas que tornam esses sistemas mais vulneráveis a ataques cibernéticos. Isso inclui todas as áreas acessíveis em que deficiências ou deficiências nos sistemas de informação (incluindo hardware, software e componentes de firmware) oferecem oportunidades para que os adversários explorem vulnerabilidades. As análises da superfície de ataque garantem que os desenvolvedores: (i) analisem as mudanças de projeto e implementação nos sistemas de informação; e (ii) mitigar os vetores de ataque gerados como resultado das mudanças. A correção de falhas identificadas inclui, por exemplo, descontinuação de funções inseguras.

### SA-11(7): Teste e Avaliação da Segurança do Desenvolvedor | Verifique o Âmbito do Ensaio/Avaliação

A organização exige que o desenvolvedor do sistema de informações, componente do sistema ou serviço do sistema de informações verifique se o escopo dos testes / avaliações de segurança oferece cobertura completa dos controles de segurança exigidos em [Atribuição: profundidade dos testes / avaliações definidos pela organização].  
Guia Adicional: A verificação de que o teste / avaliação de segurança fornece cobertura completa dos controles de segurança necessários pode ser realizada por uma variedade de técnicas analíticas, variando de informal a formal. Cada uma dessas técnicas fornece um nível crescente de garantia correspondente ao grau de formalidade da análise. A demonstração rigorosa da cobertura do controle de segurança nos níveis mais altos de garantia pode ser fornecida pelo uso de técnicas formais de modelagem e análise, incluindo correlação entre a implementação do controle e os casos de teste correspondentes.

### SA-11(8): Teste e Avaliação da Segurança do Desenvolvedor | Análise do Código Dinâmico

A organização exige que o desenvolvedor do sistema de informações, componente do sistema ou serviço do sistema de informações empregue ferramentas dinâmicas de análise de código para identificar falhas comuns e documentar os resultados da análise.  
Guia Adicional: A análise dinâmica de código fornece verificação em tempo de execução de programas de software, usando ferramentas capazes de monitorar programas quanto à corrupção de memória, problemas de privilégios do usuário e outros possíveis problemas de segurança. A análise dinâmica de código emprega ferramentas de tempo de execução para ajudar a garantir que a funcionalidade de segurança funcione da maneira como foi projetada. Um tipo especializado de análise dinâmica, conhecido como teste de fuzz, induz falhas de programa ao introduzir deliberadamente dados malformados ou aleatórios em programas de software. As estratégias de teste de fuzz derivam do uso pretendido dos aplicativos e das especificações funcionais e de design dos aplicativos. Para entender o escopo da análise dinâmica de código e, portanto, a garantia fornecida, as organizações também podem considerar a realização de uma análise de cobertura de código (verificar o grau em que o código foi testado usando métricas como porcentagem de sub-rotinas testadas ou porcentagem de instruções do programa chamadas durante a execução de a suíte de testes) e/ou análise de concordância (verificação de palavras que estão fora do lugar no código do software, como palavras em inglês ou termos depreciativos).

**Referências:**

|  |  |
| --- | --- |
| ISO 15408 | http://www.iso.org/iso/iso\_catalogue/catalogue\_tc/catalogue\_detail.htm?csnumber=50341 |
| Publicação Especial NIST 800-53A | https://csrc.nist.gov/publications/search?keywords-lg=800-53A |
| NIST - NVD: Banco de Dados Nacional de Vulnerabilidades | http://nvd.nist.gov |
| CWE: Enumeração de Fraqueza Comum | http://cwe.mitre.org |
| CVE: Vulnerabilidades e Exposições Comuns | http://cve.mitre.org |
| CAPEC: Enumeração e Classificação do Padrão de Ataque Comum | http://capec.mitre.org |

## SA-12: Proteção da Corrente de Fornecimento (P1)

**Descrição do Controle:**A organização protege contra ameaças da cadeia de suprimentos ao sistema de informação, componente do sistema ou serviço do sistema de informação, empregando [Atribuição: salvaguardas de segurança definidas pela organização] como parte de uma estratégia abrangente de segurança da informação de defesa abrangente.  
  
**Guia Adicional:**Os sistemas de informação (incluindo componentes do sistema que compõem esses sistemas) precisam ser protegidos durante todo o ciclo de vida do desenvolvimento do sistema (ou seja, durante o design, desenvolvimento, fabricação, embalagem, montagem, distribuição, integração do sistema, operações, manutenção e desativação). A proteção dos sistemas de informações organizacionais é realizada por meio da conscientização de ameaças, pela identificação, gerenciamento e redução de vulnerabilidades em cada fase do ciclo de vida e pelo uso de estratégias complementares que se reforçam mutuamente para responder aos riscos. As organizações consideram a implementação de um processo padronizado para lidar com os riscos da cadeia de suprimentos com relação aos sistemas de informação e componentes do sistema e educar a força de trabalho de aquisição sobre ameaças, riscos e controles de segurança necessários. As organizações usam os processos de aquisição / aquisição para exigir que as entidades da cadeia de suprimentos implementem as salvaguardas de segurança necessárias para: (i) reduzir a probabilidade de modificações não autorizadas em cada estágio da cadeia de suprimentos; e (ii) proteger os sistemas de informação e os componentes do sistema de informação antes de receber esses sistemas / componentes. Esse controle também se aplica aos serviços do sistema de informações. As salvaguardas de segurança incluem, por exemplo: (i) controles de segurança para sistemas de desenvolvimento, instalações de desenvolvimento e conexões externas a sistemas de desenvolvimento; (ii) examinar o pessoal de desenvolvimento; e (iii) uso de embalagem inviolável durante o transporte / armazenamento. Os métodos para revisar e proteger os planos, evidências e documentação de desenvolvimento são proporcionais à categoria de segurança ou ao nível de classificação do sistema de informações. Os contratos podem especificar requisitos de proteção da documentação.  
  
**Melhorias do Controle:**

### SA-12(1): Proteção da Corrente de Fornecimento | Estratégias / Ferramentas / Métodos de Aquisição

A organização emprega [Atribuição: estratégias de aquisição definidas pela organização, ferramentas de contrato e métodos de aquisição] para a compra do sistema de informações, componente do sistema ou serviço do sistema de informações dos fornecedores.  
Guia Adicional: O uso dos processos de aquisição e aquisição pelas organizações no início do ciclo de vida de desenvolvimento do sistema fornece um veículo importante para proteger a cadeia de suprimentos. As organizações usam a análise de inteligência de todas as fontes disponíveis para informar a adaptação de estratégias, ferramentas e métodos de aquisição. Existem várias ferramentas e técnicas diferentes disponíveis (por exemplo, obscurecer o uso final de um sistema de informações ou componente do sistema, usando compras ocultas ou filtradas). As organizações também consideram criar incentivos para fornecedores que: (i) implementam as salvaguardas de segurança necessárias; (ii) promover a transparência em seus processos organizacionais e práticas de segurança; (iii) fornecer verificação adicional dos processos e práticas de segurança de fornecedores subordinados, componentes críticos do sistema de informações e serviços; (iv) restringir compras de fornecedores ou países específicos; e (v) fornecer a linguagem do contrato referente à proibição de componentes contaminados ou falsificados. Além disso, as organizações consideram minimizar o tempo entre as decisões de compra e a entrega necessária para limitar as oportunidades dos adversários de corromper componentes ou produtos do sistema de informações. Finalmente, as organizações podem usar opções confiáveis / controladas de distribuição, entrega e armazenamento para reduzir o risco da cadeia de suprimentos (por exemplo, exigindo embalagem inviolável dos componentes do sistema de informações durante o transporte e o armazenamento).

### SA-12(2): Proteção da Corrente de Fornecimento | Avaliações do Fornecedor

A organização realiza uma revisão de fornecedor antes de celebrar um contrato para adquirir o sistema de informações, o componente do sistema ou o serviço do sistema de informações.  
Guia Adicional: As análises de fornecedores incluem, por exemplo: (i) análise de processos de fornecedores usados para projetar, desenvolver, testar, implementar, verificar, entregar e dar suporte a sistemas de informação, componentes de sistema e serviços de sistema de informação; e (ii) avaliação do treinamento e da experiência do fornecedor no desenvolvimento de sistemas, componentes ou serviços com a capacidade de segurança necessária. Essas análises fornecem às organizações níveis aumentados de visibilidade das atividades do fornecedor durante o ciclo de vida de desenvolvimento do sistema para promover um gerenciamento mais eficaz dos riscos da cadeia de suprimentos. As análises de fornecedores também podem ajudar a determinar se os fornecedores principais possuem salvaguardas de segurança e uma prática para verificar fornecedores subordinados, por exemplo, fornecedores de segundo e terceiro níveis e quaisquer subcontratados.

### SA-12(3): Proteção da Corrente de Fornecimento | Transporte Confiável e Armazenagem

[Retirado: Incorporado na SA-12 (1)].

### SA-12(4): Proteção da Corrente de Fornecimento | Diversidade de Fornecedores

[Retirado: Incorporado na SA-12 (13)].

### SA-12(5): Proteção da Corrente de Fornecimento | Limitação de Danos

A organização emprega [Atribuição: salvaguardas de segurança definidas pela organização] para limitar os danos de adversários em potencial que identificam e direcionam a cadeia de suprimentos organizacional.  
Guia Adicional: O risco da cadeia de suprimentos faz parte da ameaça persistente avançada (APT). As salvaguardas e contramedidas de segurança para reduzir a probabilidade de adversários identificarem e direcionarem com êxito a cadeia de suprimentos incluem, por exemplo: (i) evitar a compra de configurações personalizadas para reduzir o risco de aquisição de sistemas de informações, componentes ou produtos que foram corrompidos por meio de suprimentos ações em cadeia direcionadas a organizações específicas; (ii) empregar um conjunto diversificado de fornecedores para limitar o dano potencial de qualquer fornecedor na cadeia de suprimentos; (iii) empregar listas de fornecedores aprovados com reputações permanentes no setor; e (iv) usar trincheiras de compras (ou seja, exclusões de compromissos ou obrigações).

### SA-12(6): Proteção da Corrente de Fornecimento | Minimizando o Tempo de Compra

[Retirado: Incorporado na SA-12 (1)].

### SA-12(7): Proteção da Corrente de Fornecimento | Avaliações Antes da Seleção / Aceitação / Atualização

A organização realiza uma avaliação do sistema de informações, componente do sistema ou serviço do sistema de informações antes da seleção, aceitação ou atualização.  
Guia Adicional: As avaliações incluem, por exemplo, testes, avaliações, revisões e análises. Entidades independentes ou de terceiros ou funcionários da organização realizam avaliações de sistemas, componentes, produtos, ferramentas e serviços. As organizações realizam avaliações para descobrir vulnerabilidades não intencionais e intencionais, incluindo, por exemplo, código malicioso, processos maliciosos, software defeituoso e falsificações. As avaliações podem incluir, por exemplo, análises estáticas, análises dinâmicas, simulações, teste de branco, cinza e caixa preta, teste de fuzz, teste de penetração e garantia de que os componentes ou serviços sejam genuínos (por exemplo, usando tags, verificações de hash criptográficas ou digitais assinaturas). As evidências geradas durante as avaliações de segurança são documentadas para ações subsequentes realizadas pelas organizações.

### SA-12(8): Proteção da Corrente de Fornecimento | Uso da Inteligência de Todas as Fontes

A organização usa análise de inteligência de todas as fontes de fornecedores e potenciais fornecedores do sistema de informação, componente do sistema ou serviço do sistema de informação.  
Guia Adicional: A análise de inteligência de todas as fontes é empregada pelas organizações para informar as decisões de engenharia, aquisição e gerenciamento de riscos. A inteligência de todas as fontes consiste em produtos e/ou organizações e atividades de inteligência que incorporam todas as fontes de informações, incluindo mais frequentemente inteligência humana, inteligência de imagens, inteligência de medição e assinatura, inteligência de sinais e inteligência de sinais e dados de código aberto na produção de inteligência finalizada. Onde disponíveis, essas informações são usadas para analisar o risco de vulnerabilidades intencionais e não intencionais dos processos de desenvolvimento, fabricação e entrega, pessoas e meio ambiente. Essa revisão é realizada em fornecedores em várias camadas da cadeia de suprimentos, suficientes para gerenciar riscos.

### SA-12(9): Proteção da Corrente de Fornecimento | Segurança das Operações

A organização emprega [Atribuição: salvaguardas de segurança operacional definidas pela organização (OPSEC)] de acordo com os guias de classificação para proteger as informações relacionadas à cadeia de suprimentos do sistema de informações, componente do sistema ou serviço do sistema de informações.  
Guia Adicional: As informações da cadeia de suprimentos incluem, por exemplo: identidades do usuário; usos para sistemas de informação, componentes de sistema de informação e serviços de sistema de informação; identidades de fornecedores; processos de fornecedores; requisitos de segurança; especificações de projeto; resultados de testes e avaliações; e configurações de sistema / componente. Esse aprimoramento de controle expande o escopo do OPSEC para incluir fornecedores e potenciais fornecedores. O OPSEC é um processo de identificação de informações críticas e subsequente análise de ações amigáveis relacionadas às operações e outras atividades para: (i) identificar as ações que podem ser observadas pelos adversários em potencial; (ii) determinar indicadores que os adversários possam obter que possam ser interpretados ou reunidos para obter informações críticas em tempo suficiente para causar danos às organizações; (iii) implementar salvaguardas ou contramedidas para eliminar ou reduzir, para um nível aceitável, vulnerabilidades exploráveis; e (iv) considerar como as informações agregadas podem comprometer a confidencialidade dos usuários ou usos da cadeia de suprimentos. O OPSEC pode exigir que as organizações retenham informações críticas de missão / negócios dos fornecedores e pode incluir o uso de intermediários para ocultar o uso final, ou usuários, de sistemas de informação, componentes de sistema ou serviços de sistema de informação.

### SA-12(10): Proteção da Corrente de Fornecimento | Validar como Genuíno e Não Alterado

A organização emprega [Atribuição: salvaguardas de segurança definidas pela organização] para validar que o sistema de informações ou componentes de sistema recebido é genuíno e não foi alterado.  
Guia Adicional: Para alguns componentes do sistema de informação, especialmente hardware, existem meios técnicos para ajudar a determinar se os componentes são genuínos ou foram alterados. As salvaguardas de segurança usadas para validar a autenticidade dos sistemas de informação e componentes do sistema de informação incluem, por exemplo, marcação óptica / nanotecnológica e análise de canal lateral. Para o hardware, as informações detalhadas da lista de materiais podem destacar os elementos com lógica incorporada completa com o local do componente e da produção.

### SA-12(11): Proteção da Corrente de Fornecimento | PenTest / Análise de Elementos, Processos e Atores

A organização emprega [Seleção (uma ou mais): análise organizacional, análise independente de terceiros, teste de penetração organizacional, teste de penetração independente de terceiros] da [Atribuição: elementos, processos e atores da cadeia de suprimentos definidos pela organização] associados ao sistema de informação, componente do sistema ou serviço do sistema de informação.  
Guia Adicional: Esse aprimoramento de controle trata da análise e/ou teste da cadeia de suprimentos, não apenas dos itens entregues. Os elementos da cadeia de suprimentos são produtos de tecnologia da informação ou componentes de produtos que contêm lógica programável e que são extremamente importantes para as funções do sistema de informação. Os processos da cadeia de suprimentos incluem, por exemplo: (i) processos de desenvolvimento de hardware, software e firmware; (ii) procedimentos de expedição / manuseio; (iii) pessoal e programas de segurança física; (iv) ferramentas / medidas de gerenciamento de configuração para manter a proveniência; ou (v) quaisquer outros programas, processos ou procedimentos associados à produção / distribuição de elementos da cadeia de suprimentos. Os atores da cadeia de suprimentos são indivíduos com funções e responsabilidades específicas na cadeia de suprimentos. As evidências geradas durante análises e testes de elementos, processos e atores da cadeia de suprimentos são documentadas e usadas para informar as atividades e decisões da gestão de riscos organizacionais.

### SA-12(12): Proteção da Corrente de Fornecimento | Acordos Entre Organizações

A organização estabelece acordos e procedimentos entre organizações com entidades envolvidas na cadeia de suprimentos do sistema de informações, componente do sistema ou serviço do sistema de informações.  
Guia Adicional: O estabelecimento de acordos e procedimentos entre organizações prevê a notificação de comprometimentos da cadeia de suprimentos. A notificação antecipada de comprometimentos da cadeia de suprimentos que podem afetar adversamente ou afetar adversamente os sistemas de informações organizacionais, incluindo componentes críticos do sistema, é essencial para que as organizações forneçam respostas apropriadas a esses incidentes.

### SA-12(13): Proteção da Corrente de Fornecimento | Componentes do Sistema de Informação Crítica

A organização emprega [Atribuição: salvaguardas de segurança definidas pela organização] para garantir um fornecimento adequado de [Atribuição: componentes do sistema de informações críticas definidas pela organização].  
Guia Adicional: Os adversários podem tentar impedir as operações organizacionais interrompendo o fornecimento de componentes críticos do sistema de informações ou corrompendo as operações do fornecedor. As salvaguardas para garantir o fornecimento adequado de componentes críticos do sistema de informações incluem, por exemplo: (i) o uso de vários fornecedores em toda a cadeia de suprimentos para os componentes críticos identificados; e (ii) armazenamento de componentes sobressalentes para garantir a operação em períodos críticos.

### SA-12(14): Proteção da Corrente de Fornecimento | Identidade e Rastreabilidade

A organização estabelece e mantém uma identificação exclusiva de [Atribuição: elementos, processos e atores da cadeia de suprimentos definidos pela organização] para o sistema de informação, componente do sistema ou serviço do sistema de informação.  
Guia Adicional: Saber quem e o que está nas cadeias de suprimentos das organizações é fundamental para obter visibilidade do que está acontecendo nessas cadeias de suprimentos, além de monitorar e identificar eventos e atividades de alto risco. Sem visibilidade e rastreabilidade razoáveis nas cadeias de suprimentos (isto é, elementos, processos e atores), é muito difícil para as organizações entenderem e, portanto, gerenciarem os riscos e reduzirem a probabilidade de eventos adversos. A identificação exclusiva das funções, organizações, pessoal, processos de missão e elemento do adquirente e integrador, procedimentos de teste e avaliação, mecanismos de entrega, mecanismos de suporte, comunicações / caminhos de entrega e atividades de descarte / disposição final, bem como os componentes e ferramentas utilizados, estabelece uma base estrutura de identidade para avaliação das atividades da cadeia de suprimentos. Por exemplo, rotular (usando números de série) e etiquetar (usando tags de identificação por radiofrequência [RFID]) elementos individuais da cadeia de suprimentos, incluindo pacotes de software, módulos e dispositivos de hardware, e processos associados a esses elementos podem ser usados para essa finalidade. Os métodos de identificação são suficientes para apoiar a proveniência no caso de um problema na cadeia de suprimentos ou um evento adverso na cadeia de suprimentos.

### SA-12(15): Proteção da Corrente de Fornecimento | Processos para Enfrentar Falhas ou Deficiências

A organização estabelece um processo para abordar deficiências ou deficiências nos elementos da cadeia de suprimentos identificados durante avaliações independentes ou organizacionais desses elementos.  
Guia Adicional: As evidências geradas durante avaliações independentes ou organizacionais dos elementos da cadeia de suprimentos (por exemplo, testes de penetração, auditorias, atividades de verificação / validação) são documentadas e usadas nos processos subsequentes implementados pelas organizações para responder aos riscos relacionados às fraquezas e deficiências identificadas. Os elementos da cadeia de suprimentos incluem, por exemplo, processos de desenvolvimento de fornecedores e sistemas de distribuição de fornecedores.

**Referências:**

|  |  |
| --- | --- |
| Publicação Especial NIST 800-161 | https://csrc.nist.gov/publications/search?keywords-lg=800-161 |
| NIST - Relatório de Interação 7622 | http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7622 |

## SA-13: Confiabilidade (P0)

**Descrição do Controle:**A organização:  
  
a. Descreve a confiabilidade exigida no [Atribuição: sistema de informações definido pela organização, componente do sistema de informações ou serviço do sistema de informações] que suporta suas missões críticas / funções de negócios; e  
  
b. Implementa [Atribuição: sobreposição de garantia definida pela organização] para alcançar tal confiabilidade.  
  
**Guia Adicional:**Esse controle ajuda as organizações a tomar decisões explícitas de confiabilidade ao projetar, desenvolver e implementar sistemas de informação necessários para conduzir missões organizacionais críticas / funções de negócios. A confiabilidade é uma característica / propriedade de um sistema de informação que expressa o grau em que se espera que o sistema preserve a confidencialidade, a integridade e a disponibilidade das informações que processa, armazena ou transmite. Sistemas de informações confiáveis são sistemas capazes de serem confiáveis para operar dentro de níveis definidos de risco, apesar das interrupções ambientais, erros humanos e ataques intencionais que se espera que ocorram nos ambientes operacionais especificados. Sistemas confiáveis são importantes para o sucesso da missão / negócios. Dois fatores que afetam a confiabilidade dos sistemas de informação incluem: (i) funcionalidade de segurança (isto é, os recursos, funções e/ou mecanismos de segurança empregados no sistema e seu ambiente de operação); e (ii) garantia de segurança (ou seja, os motivos de confiança de que a funcionalidade de segurança é eficaz em sua aplicação). Desenvolvedores, implementadores, operadores e mantenedores de sistemas de informações organizacionais podem aumentar o nível de garantia (e confiabilidade), por exemplo, empregando modelos de política de segurança bem definidos, técnicas de desenvolvimento de hardware, software e firmware estruturado e rigoroso, técnicas de desenvolvimento de hardware, software e firmware, sistema de som / princípios de engenharia de segurança e definições de configuração segura (definidas por um conjunto de controles de segurança relacionados à garantia no Apêndice E). A garantia também se baseia na avaliação das evidências produzidas durante o ciclo de vida de desenvolvimento do sistema. As missões críticas / funções de negócios são suportadas por sistemas de alto impacto e pelos requisitos de garantia associados a esses sistemas. Os controles adicionais de garantia na Tabela E-4 no Apêndice E (designados como opcionais) podem ser usados para desenvolver e implementar soluções de alta garantia para sistemas de informações e componentes de sistemas específicos, usando o conceito de sobreposições descrito no Apêndice I. As organizações selecionam sobreposições de garantia que foram desenvolvidos, validados e aprovados para adoção pela comunidade (por exemplo, entre organizações, em todo o governo), limitando o desenvolvimento de tais sobreposições em uma organização por organização. As organizações podem realizar análises de criticidade, conforme descrito na SA-14, para determinar os sistemas de informação, componentes de sistema ou serviços de sistema de informação que requerem soluções de alta garantia. Os requisitos de confiabilidade e as sobreposições de garantia podem ser descritos nos planos de segurança dos sistemas de informações organizacionais.

**Referências:**

|  |  |
| --- | --- |
| Publicações de Normas Federais de Processamento de Informações N.199 | http://csrc.nist.gov/publications/PubsFIPS.html#199 |
| Publicações de Normas Federais de Processamento de Informações N.200 | http://csrc.nist.gov/publications/PubsFIPS.html#200 |
| Publicação Especial NIST 800-53 | https://csrc.nist.gov/publications/search?keywords-lg=800-53 |
| Publicação Especial NIST 800-60 | https://csrc.nist.gov/publications/search?keywords-lg=800-60 |
| Publicação Especial NIST 800-64 | https://csrc.nist.gov/publications/search?keywords-lg=800-64 |

## SA-14: Análise Crítica (P0)

**Descrição do Controle:**A organização identifica componentes e funções críticas do sistema de informação executando uma análise de criticidade para [Atribuição: sistemas de informação definidos pela organização, componentes de sistema de informação ou serviços de sistema de informação] em [Atribuição: pontos de decisão definidos pela organização no ciclo de vida de desenvolvimento do sistema].  
  
**Guia Adicional:**A análise de criticidade é um princípio essencial do gerenciamento de riscos da cadeia de suprimentos e informa a priorização de atividades de proteção da cadeia de suprimentos, como redução da superfície de ataque, uso de inteligência de todas as fontes e estratégias de aquisição personalizadas. Os engenheiros de sistemas de informação podem conduzir uma decomposição funcional de ponta a ponta de um sistema de informações para identificar funções e componentes de missão crítica. A decomposição funcional inclui a identificação das principais missões organizacionais suportadas pelo sistema, a decomposição nas funções específicas para executar essas missões e a rastreabilidade aos componentes de hardware, software e firmware que implementam essas funções, incluindo quando as funções são compartilhadas por muitos componentes dentro e além do limite do sistema de informação. Os componentes do sistema de informações que permitem acesso não mediado a componentes ou funções críticas são considerados críticos devido às vulnerabilidades inerentes que esses componentes criam. A criticidade é avaliada em termos do impacto da função ou falha do componente na capacidade do componente de completar as missões organizacionais suportadas pelo sistema de informação. Uma análise de criticidade é realizada sempre que uma arquitetura ou design está sendo desenvolvido ou modificado, incluindo atualizações.  
  
**Melhorias do Controle:**

### SA-14(1): Análise Crítica | Componentes Críticos, Sem Fonte Alternativa Viável

[Retirado: Incorporado na SA-20].

## SA-15: Processo de Desenvolvimento, Normas e Ferramentas (P2)

**Descrição do Controle:**A organização:  
  
a. Requer que o desenvolvedor do sistema de informações, componente do sistema ou serviço do sistema de informações siga um processo de desenvolvimento documentado que:  
  
1. Aborde explicitamente os requisitos de segurança;  
  
2. Identifica os padrões e ferramentas utilizados no processo de desenvolvimento;  
  
3. Documenta as opções específicas da ferramenta e as configurações da ferramenta usadas no processo de desenvolvimento; e  
  
4. Documenta, gerencia e garante a integridade das alterações no processo e/ou ferramentas usadas no desenvolvimento; e  
  
b. Revisa o processo de desenvolvimento, padrões, ferramentas e opções / configurações de ferramentas [Atribuição: frequência definida pela organização] para determinar se o processo, padrões, ferramentas e opções / configurações de ferramentas selecionadas e empregadas podem satisfazer [Atribuição: requisitos de segurança definidos pela organização ]  
  
**Guia Adicional:**As ferramentas de desenvolvimento incluem, por exemplo, linguagens de programação e sistemas de desenho auxiliado por computador (CAD). As revisões dos processos de desenvolvimento podem incluir, por exemplo, o uso de modelos de maturidade para determinar a eficácia potencial de tais processos. Manter a integridade das alterações nas ferramentas e processos permite uma avaliação e mitigação precisas dos riscos da cadeia de suprimentos e requer um controle de configuração robusto ao longo do ciclo de vida (incluindo design, desenvolvimento, transporte, entrega, integração e manutenção) para rastrear alterações autorizadas e impedir alterações não autorizadas .  
  
**Melhorias do Controle:**

### SA-15(1): Processo de Desenvolvimento, Normas e Ferramentas | Processo de Desenvolvimento, Métricas de Qualidade

A organização exige que o desenvolvedor do sistema de informações, componente do sistema ou serviço do sistema de informações:  
  
a. Definir métricas de qualidade no início do processo de desenvolvimento; e  
  
b. Fornecer evidências de atendimento às métricas de qualidade [Seleção (uma ou mais): [Tarefa: frequência definida pela organização]; [Tarefa: marcos da revisão do programa definido pela organização]; na entrega].  
Guia Adicional: As organizações usam métricas de qualidade para estabelecer níveis mínimos aceitáveis de qualidade do sistema de informação. As métricas podem incluir portas de qualidade, que são coleções de critérios de conclusão ou padrões de suficiência que representam a execução satisfatória de fases específicas do projeto de desenvolvimento do sistema. Um portal de qualidade, por exemplo, pode exigir a eliminação de todos os avisos do compilador ou uma determinação explícita de que os avisos não têm impacto na eficácia dos recursos de segurança necessários. Durante as fases de execução dos projetos de desenvolvimento, os portões da qualidade fornecem indicações claras e inequívocas de progresso. Outras métricas se aplicam a todo o projeto de desenvolvimento. Essas métricas podem incluir a definição dos limites de severidade das vulnerabilidades, por exemplo, não exigindo vulnerabilidades conhecidas no sistema de informações entregues com uma severidade Média ou Alta de Sistema de pontuação de vulnerabilidade comum (CVSS).

### SA-15(2): Processo de Desenvolvimento, Normas e Ferramentas | Processo de Desenvolvimento, Ferramentas de Segurança

A organização exige que o desenvolvedor do sistema de informações, componente do sistema ou serviço do sistema de informações selecione e empregue uma ferramenta de rastreamento de segurança para uso durante o processo de desenvolvimento.  
Guia Adicional: As equipes de desenvolvimento de sistemas de informação selecionam e implantam ferramentas de rastreamento de segurança, incluindo, por exemplo, sistemas de rastreamento de itens de trabalho / vulnerabilidade que facilitam a atribuição, classificação, filtragem e rastreamento de itens de trabalho concluídos ou tarefas associadas aos processos de desenvolvimento do sistema.

### SA-15(3): Processo de Desenvolvimento, Normas e Ferramentas | Processo de Desenvolvimento, Análise de Crítica

A organização exige que o desenvolvedor do sistema de informações, componente do sistema ou serviço do sistema de informações realize uma análise de criticidade em [Atribuição: largura / profundidade definida pela organização] e em [Atribuição: pontos de decisão definidos pela organização no ciclo de vida de desenvolvimento do sistema] .  
Guia Adicional: Esse aprimoramento de controle fornece informações do desenvolvedor para a análise de criticidade realizada pelas organizações no SA-14. A contribuição do desenvolvedor é essencial para essa análise, porque as organizações podem não ter acesso a documentação detalhada do projeto para os componentes do sistema de informação que são desenvolvidos como produtos comerciais de tecnologia da informação disponíveis no mercado (COTS) (por exemplo, especificações funcionais, projetos de alto nível, baixo custo). projetos de nível e esquemas de código-fonte / hardware).

### SA-15(4): Processo de Desenvolvimento, Normas e Ferramentas | Processo de Desenvolvimento, Modelagem de Ameaças / Análise de Vulnerabilidade

A organização exige que os desenvolvedores realizem modelagem de ameaças e uma análise de vulnerabilidade para o sistema de informações em [Atribuição: amplitude / profundidade definida pela organização] que:  
  
a. Usos [Atribuição: informações definidas pela organização sobre impacto, ambiente de operações, ameaças conhecidas ou assumidas e níveis de risco aceitáveis];  
  
b. Emprega [atribuição: ferramentas e métodos definidos pela organização]; e  
  
c. Produz evidências que atendem [Atribuição: critérios de aceitação definidos pela organização].

### SA-15(5): Processo de Desenvolvimento, Normas e Ferramentas | Processo de Desenvolvimento, Redução de Superfície de Ataque

A organização exige que o desenvolvedor do sistema de informações, componente do sistema ou serviço do sistema de informações reduza as superfícies de ataque para [Atribuição: limites definidos pela organização].  
Guia Adicional: A redução da superfície de ataque está alinhada com as análises de ameaças e vulnerabilidades do desenvolvedor e a arquitetura e o design do sistema de informação. A redução da superfície de ataque é um meio de reduzir o risco para as organizações, oferecendo aos atacantes menos oportunidade de explorar pontos fracos ou deficiências (ou seja, possíveis vulnerabilidades) nos sistemas de informação, componentes do sistema de informação e serviços do sistema de informação. A redução da superfície de ataque inclui, por exemplo, a aplicação do princípio de menor privilégio, o emprego de defesas em camadas, a aplicação do princípio de menor funcionalidade (ou seja, restrição de portas, protocolos, funções e serviços, descontinuação de funções inseguras e eliminação de interfaces de programação de aplicativos APIs) vulneráveis a ataques cibernéticos.

### SA-15(6): Processo de Desenvolvimento, Normas e Ferramentas | Processo de Desenvolvimento, Melhoria Continua

A organização exige que o desenvolvedor do sistema de informações, componente do sistema ou serviço do sistema de informações implemente um processo explícito para melhorar continuamente o processo de desenvolvimento.  
Guia Adicional: Os desenvolvedores de sistemas de informação, componentes de sistema de informação e serviços de sistema de informação consideram a eficácia / eficiência dos processos de desenvolvimento atuais para atender aos objetivos de qualidade e abordar os recursos de segurança nos ambientes de ameaças atuais.

### SA-15(7): Processo de Desenvolvimento, Normas e Ferramentas | Processo de Desenvolvimento, Análise Automatizada de Vulnerabilidade

A organização exige que o desenvolvedor do sistema de informações, componente do sistema ou serviço do sistema de informações:  
  
a. Execute uma análise automatizada de vulnerabilidades usando [Atribuição: ferramentas definidas pela organização];  
  
b. Determine o potencial de exploração de vulnerabilidades descobertas;  
  
c. Determinar possíveis atenuações de riscos para vulnerabilidades entregues; e  
  
d. Entregue os resultados das ferramentas e dos resultados da análise para [Atribuição: pessoal ou funções definidas pela organização].

### SA-15(8): Processo de Desenvolvimento, Normas e Ferramentas | Processo de Desenvolvimento, Reutilização de Informações de Ameaça/Vulnerabilidade

A organização exige que o desenvolvedor do sistema de informações, componente do sistema ou serviço do sistema de informações use modelagem de ameaças e análises de vulnerabilidade de sistemas, componentes ou serviços similares para informar o processo de desenvolvimento atual.  
Guia Adicional: A análise de vulnerabilidades encontradas em aplicativos de software semelhantes pode informar possíveis problemas de design ou implementação de sistemas de informação em desenvolvimento. Sistemas de informação ou componentes de sistema semelhantes podem existir nas organizações de desenvolvedores. Informações de vulnerabilidade autorizadas estão disponíveis em várias fontes do setor público e privado, incluindo, por exemplo, o Banco de Dados Nacional de Vulnerabilidades.

### SA-15(9): Processo de Desenvolvimento, Normas e Ferramentas | Processo de Desenvolvimento, Uso de Dados ao Vivo

A organização aprova, documenta e controla o uso de dados ativos em ambientes de desenvolvimento e teste para o sistema de informações, componente do sistema ou serviço do sistema de informações.  
Guia Adicional: O uso de dados ativos em ambientes de pré-produção pode resultar em riscos significativos para as organizações. As organizações podem minimizar esse risco usando dados de teste ou fictícios durante o desenvolvimento e teste de sistemas de informação, componentes de sistema de informação e serviços de sistema de informação.

### SA-15(10): Processo de Desenvolvimento, Normas e Ferramentas | Processo de Desenvolvimento, Plano de Resposta a Incidentes

A organização exige que o desenvolvedor do sistema de informações, componente do sistema ou serviço do sistema de informações forneça um plano de resposta a incidentes.  
Guia Adicional: O plano de resposta a incidentes para desenvolvedores de sistemas de informações, componentes de sistema e serviços de sistemas de informações é incorporado aos planos organizacionais de resposta a incidentes para fornecer o tipo de informações de resposta a incidentes que não estão prontamente disponíveis para as organizações. Essas informações podem ser extremamente úteis, por exemplo, quando as organizações respondem a vulnerabilidades em produtos comerciais de tecnologia da informação disponíveis no mercado (COTS).

### SA-15(11): Processo de Desenvolvimento, Normas e Ferramentas | Processo de Desenvolvimento, Sistema de Informação / Componente de Arquivo

A organização exige que o desenvolvedor do sistema de informações ou componente do sistema arquive o sistema ou componente a ser liberado ou entregue juntamente com as evidências correspondentes que suportam a revisão final de segurança.  
Guia Adicional: O arquivamento de documentação relevante do processo de desenvolvimento pode fornecer uma linha de base de informações prontamente disponíveis, que pode ser útil durante as atualizações ou modificações do sistema de informações / componentes.

## SA-16: Formação Fornecida pelo Desenvolvedor (P2)

**Descrição do Controle:**A organização exige que o desenvolvedor do sistema de informações, componente do sistema ou serviço do sistema de informações forneça [Atribuição: treinamento definido pela organização] sobre o uso e operação corretos das funções, controles e/ou mecanismos de segurança implementados.  
  
**Guia Adicional:**Esse controle se aplica a desenvolvedores externos e internos (internos). O treinamento de pessoal é um elemento essencial para garantir a eficácia dos controles de segurança implementados nos sistemas de informações organizacionais. As opções de treinamento incluem, por exemplo, treinamento em sala de aula, treinamento baseado na Web / computador e treinamento prático. As organizações também podem solicitar materiais de treinamento suficientes dos desenvolvedores para realizar o treinamento interno ou oferecer auto-treinamento ao pessoal da organização. As organizações determinam o tipo de treinamento necessário e podem exigir diferentes tipos de treinamento para diferentes funções, controles ou mecanismos de segurança.

## SA-17: Arquitetura e Design de Segurança do Desenvolvedor (P1)

**Descrição do Controle:**A organização exige que o desenvolvedor do sistema de informações, componente do sistema ou serviço do sistema de informações produza uma especificação de design e arquitetura de segurança que:  
  
a. É consistente e apoia a arquitetura de segurança da organização, que é estabelecida dentro e é parte integrante da arquitetura corporativa da organização;  
  
b. Descreve com precisão e completamente a funcionalidade de segurança necessária e a alocação de controles de segurança entre componentes físicos e lógicos; e  
  
c. Expressa como funções, mecanismos e serviços de segurança individuais trabalham juntos para fornecer os recursos de segurança necessários e uma abordagem unificada da proteção.  
  
**Guia Adicional:**Esse controle é direcionado principalmente a desenvolvedores externos, embora também possa ser usado para desenvolvimento interno (interno). Por outro lado, o PL-8 é direcionado principalmente a desenvolvedores internos para ajudar a garantir que as organizações desenvolvam uma arquitetura de segurança da informação e essa arquitetura de segurança seja integrada ou fortemente acoplada à arquitetura corporativa. Essa distinção é importante se / quando as organizações terceirizam o desenvolvimento de sistemas de informação, componentes de sistema de informação ou serviços de sistema de informação para entidades externas, e há um requisito para demonstrar consistência com a arquitetura corporativa da organização e a arquitetura de segurança da informação.  
  
**Melhorias do Controle:**

### SA-17(1): Arquitetura e Design de Segurança do Desenvolvedor | Modelo de Política Formal

A organização exige que o desenvolvedor do sistema de informações, componente do sistema ou serviço do sistema de informações:  
  
a. Produzir, como parte integrante do processo de desenvolvimento, um modelo formal de política que descreva os [Atribuição: elementos definidos pela organização da política de segurança organizacional] a serem aplicados; e  
  
b. Prove que o modelo de política formal é internamente consistente e suficiente para impor os elementos definidos da política de segurança organizacional quando implementada.  
Guia Adicional: Os modelos formais descrevem comportamentos ou políticas de segurança específicos usando linguagens formais, permitindo assim que a correção desses comportamentos / políticas seja formalmente comprovada. Nem todos os componentes dos sistemas de informação podem ser modelados e, geralmente, as especificações formais têm como escopo comportamentos específicos ou políticas de interesse (por exemplo, políticas de controle de acesso não discricionárias). As organizações escolhem a linguagem de modelagem formal específica e a abordagem com base na natureza dos comportamentos / políticas a serem descritas e nas ferramentas disponíveis. Ferramentas de modelagem formais incluem, por exemplo, Gypsy e Zed.

### SA-17(2): Arquitetura e Design de Segurança do Desenvolvedor | Componentes Relevantes da Segurança

A organização exige que o desenvolvedor do sistema de informações, componente do sistema ou serviço do sistema de informações:  
  
a. Definir hardware, software e firmware relevantes à segurança; e  
  
b. Forneça uma justificativa para que a definição de hardware, software e firmware relevante para a segurança esteja completa.  
Guia Adicional: O hardware, software e firmware relevantes à segurança representam a parte do sistema, componente ou serviço de informações em que deve ser confiável o desempenho correto para manter as propriedades de segurança necessárias.

### SA-17(3): Arquitetura e Design de Segurança do Desenvolvedor | Correspondência Formal

A organização exige que o desenvolvedor do sistema de informações, componente do sistema ou serviço do sistema de informações:  
  
a. Produzir, como parte integrante do processo de desenvolvimento, uma especificação formal de nível superior que especifique as interfaces para hardware, software e firmware relevantes à segurança em termos de exceções, mensagens de erro e efeitos;  
  
b. Mostrar, por meio de provas, na medida do possível, com a demonstração informal adicional, conforme necessário, que a especificação formal de nível superior é consistente com o modelo formal de política;  
  
c. Mostrar por demonstração informal, que a especificação formal de nível superior cobre completamente as interfaces para hardware, software e firmware relevantes à segurança;  
  
d. Mostre que a especificação formal de nível superior é uma descrição precisa do hardware, software e firmware implementados relevantes para a segurança; e  
  
e. Descreva os mecanismos de hardware, software e firmware relevantes à segurança, não abordados na especificação formal de nível superior, mas estritamente internos ao hardware, software e firmware relevantes à segurança.  
Guia Adicional: A correspondência é uma parte importante da garantia obtida com a modelagem. Isso demonstra que a implementação é uma transformação precisa do modelo e que qualquer código adicional ou detalhes de implementação presentes não têm impacto nos comportamentos ou políticas que estão sendo modelados. Métodos formais podem ser usados para mostrar que as propriedades de segurança de alto nível são satisfeitas pela descrição formal do sistema de informações e que a descrição formal do sistema é implementada corretamente por uma descrição de algum nível inferior, por exemplo, uma descrição de hardware. A consistência entre a especificação formal de nível superior e os modelos de políticas formais geralmente não é passível de ser totalmente comprovada. Portanto, pode ser necessária uma combinação de métodos formais / informais para mostrar essa consistência. A consistência entre a especificação formal de nível superior e a implementação pode exigir o uso de uma demonstração informal devido a limitações na aplicabilidade de métodos formais para provar que a especificação reflete com precisão a implementação. Os mecanismos de hardware, software e firmware estritamente internos ao hardware, software e firmware relevantes à segurança incluem, por exemplo, registros de mapeamento e entrada / saída direta de memória.

### SA-17(4): Arquitetura e Design de Segurança do Desenvolvedor | Correspondência Informal

A organização exige que o desenvolvedor do sistema de informações, componente do sistema ou serviço do sistema de informações:  
  
a. Produzir, como parte integrante do processo de desenvolvimento, uma especificação descritiva informal de nível superior que especifique as interfaces para hardware, software e firmware relevantes à segurança em termos de exceções, mensagens de erro e efeitos;  
  
b. Mostrar via [Seleção: demonstração informal, argumento convincente com métodos formais possível] que a especificação descritiva de nível superior é consistente com o modelo formal de política;  
  
c. Mostrar por demonstração informal, que a especificação descritiva de nível superior cobre completamente as interfaces para hardware, software e firmware relevantes para a segurança;  
  
d. Mostre que a especificação descritiva de nível superior é uma descrição precisa das interfaces para hardware, software e firmware relevantes à segurança; e  
  
e. Descreva os mecanismos de hardware, software e firmware relevantes à segurança, não abordados na especificação descritiva de nível superior, mas estritamente internos ao hardware, software e firmware relevantes à segurança.  
Guia Adicional: A correspondência é uma parte importante da garantia obtida com a modelagem. Isso demonstra que a implementação é uma transformação precisa do modelo e que qualquer código adicional ou detalhes de implementação presentes não têm impacto nos comportamentos ou políticas que estão sendo modelados. A consistência entre a especificação descritiva de nível superior (design de alto nível / baixo nível) e o modelo formal de política geralmente não é passível de ser totalmente comprovada. Portanto, pode ser necessária uma combinação de métodos formais / informais para mostrar essa consistência. Os mecanismos de hardware, software e firmware estritamente internos ao hardware, software e firmware relevantes à segurança incluem, por exemplo, registros de mapeamento e entrada / saída direta de memória.

### SA-17(5): Arquitetura e Design de Segurança do Desenvolvedor | Projeto Conceitualmente Simples

A organização exige que o desenvolvedor do sistema de informações, componente do sistema ou serviço do sistema de informações:  
  
a. Projetar e estruturar o hardware, software e firmware relevantes à segurança para usar um mecanismo de proteção completo, conceitualmente simples, com semântica definida com precisão; e  
  
b. Estruture internamente o hardware, software e firmware relevantes à segurança, com atenção específica a esse mecanismo.

### SA-17(6): Arquitetura e Design de Segurança do Desenvolvedor | Estrutura para Ensaio

A organização exige que o desenvolvedor do sistema de informações, componente do sistema ou serviço do sistema de informações estruture o hardware, software e firmware relevantes à segurança para facilitar o teste.

### SA-17(7): Arquitetura e Design de Segurança do Desenvolvedor | Estrutura para Menor Privilégio

A organização exige que o desenvolvedor do sistema de informações, componente do sistema ou serviço do sistema de informações estruture o hardware, software e firmware relevantes à segurança para facilitar o controle do acesso com o mínimo de privilégios.

## SA-18: Resistência e Detecção de Manipulação (P0)

**Descrição do Controle:**A organização implementa um programa de proteção contra adulteração para o sistema de informações, componente do sistema ou serviço do sistema de informações.  
  
**Guia Adicional:**As tecnologias e técnicas anti-adulteração fornecem um nível de proteção para sistemas críticos de informação, componentes de sistema e produtos de tecnologia da informação contra várias ameaças relacionadas, incluindo modificação, engenharia reversa e substituição. Uma identificação forte combinada com resistência à violação e/ou detecção de violação é essencial para proteger sistemas de informação, componentes e produtos durante a distribuição e quando em uso.  
  
**Melhorias do Controle:**

### SA-18(1): Resistência e Detecção de Manipulação | Várias Fases do SDLC

A organização emprega tecnologias e técnicas anti-adulteração durante várias fases do ciclo de vida de desenvolvimento do sistema, incluindo design, desenvolvimento, integração, operações e manutenção.  
Guia Adicional: As organizações usam uma combinação de técnicas de hardware e software para resistência e detecção de violações. As organizações empregam ofuscação e auto verificação, por exemplo, para tornar a engenharia reversa e as modificações mais difíceis, demoradas e caras para os adversários. A personalização dos sistemas de informação e dos componentes do sistema pode facilitar a detecção de substituições e, portanto, limitar os danos.

### SA-18(2): Resistência e Detecção de Manipulação | Inspeção de Sistemas de Informação, Componentes ou Dispositivos

A organização inspeciona [Atribuição: sistemas de informação definidos pela organização, componentes do sistema ou dispositivos] [Seleção (um ou mais): aleatoriamente; em [Atribuição: frequência definida pela organização], em [Atribuição: indicações definidas pela organização de necessidade de inspeção]] para detectar adulteração.  
Guia Adicional: Esse aprimoramento de controle aborda violações físicas e lógicas e normalmente é aplicado a dispositivos móveis, notebooks ou outros componentes do sistema retirados de áreas controladas pela organização. As indicações de necessidade de inspeção incluem, por exemplo, quando os indivíduos retornam da viagem para locais de alto risco.

## SA-19: Autenticidade do Componente (P0)

**Descrição do Controle:**A organização:  
  
a. Desenvolve e implementa políticas e procedimentos antifalsificação que incluem os meios para detectar e impedir a entrada de componentes falsificados no sistema de informação; e  
  
b. Relata componentes do sistema de informações falsas para [Seleção (um ou mais): fonte do componente falsificado; [Atribuição: organizações de relatórios externos definidas pela organização]; [Designação: pessoal ou funções definidas pela organização]].  
  
**Guia Adicional:**As fontes de componentes falsificados incluem, por exemplo, fabricantes, desenvolvedores, fornecedores e contratados. A política e os procedimentos antifalsificação suportam a resistência a violações e fornecem um nível de proteção contra a introdução de código malicioso. As organizações de relatórios externos incluem, por exemplo, US-CERT.  
  
**Melhorias do Controle:**

### SA-19(1): Autenticidade do Componente | Treinamento Anti-Falsificação

A organização treina [Designação: pessoal ou funções definidas pela organização] para detectar componentes do sistema de informações falsas (incluindo hardware, software e firmware).

### SA-19(2): Autenticidade do Componente | Controle de Configuração para Serviços / Reparos de Componentes

A organização mantém controle de configuração sobre [Atribuição: componentes do sistema de informações definidos pela organização] aguardando serviço / reparo e componentes com serviço / reparados aguardando retorno ao serviço.

### SA-19(3): Autenticidade do Componente | Eliminação do Componente

A organização descarta os componentes do sistema de informações usando [Atribuição: técnicas e métodos definidos pela organização].  
Guia Adicional: O descarte adequado dos componentes do sistema de informações ajuda a impedir que esses componentes entrem no mercado cinza.

### SA-19(4): Autenticidade do Componente | Análise Contra Falsificação

A organização verifica os componentes do sistema de informações falsas [Atribuição: frequência definida pela organização].

## SA-20: Desenvolvimento Personalizado de Componentes Críticos (P0)

**Descrição do Controle:**A organização reimplementa ou desenvolve [Atribuição: componentes do sistema de informações críticas definidas pela organização].  
  
**Guia Adicional:**As organizações determinam que certos componentes do sistema de informação provavelmente não podem ser confiáveis devido a ameaças e vulnerabilidades específicas nesses componentes e para os quais não há controles de segurança viáveis para mitigar adequadamente o risco resultante. A reimplementação ou desenvolvimento personalizado desses componentes ajuda a satisfazer os requisitos de maior segurança. Isso é realizado iniciando alterações nos componentes do sistema (incluindo hardware, software e firmware), de modo que os ataques padrão dos adversários têm menos probabilidade de êxito. Em situações em que nenhuma fonte alternativa está disponível e as organizações optam por não reimplementar ou desenvolver componentes críticos do sistema de informações, salvaguardas adicionais podem ser empregadas (por exemplo, auditoria aprimorada, restrições no código-fonte e acesso aos utilitários do sistema e proteção contra exclusão do sistema e arquivos de aplicativos.

## SA-21: Triagem de Desenvolvedores (P0)

**Descrição do Controle:**A organização exige que o desenvolvedor de [Atribuição: sistema de informações definido pela organização, componente do sistema ou serviço do sistema de informações]:  
  
a. Ter autorizações de acesso apropriadas, conforme determinado por [Atribuição: deveres oficiais do governo definidos pela organização]; e  
  
b. Satisfazer [Tarefa: critérios de triagem de pessoal adicional definidos pela organização].  
  
**Guia Adicional:**Como o sistema de informações, o componente do sistema ou o serviço do sistema de informações podem ser empregados em atividades críticas essenciais aos interesses nacionais e/ou de segurança econômica dos Estados Unidos, as organizações têm um forte interesse em garantir que o desenvolvedor seja confiável. O grau de confiança exigido do desenvolvedor pode precisar ser consistente com o das pessoas que acessam o sistema de informações / componente / serviço após a implantação. Exemplos de critérios de autorização e triagem de pessoal incluem liberação, verificações satisfatórias de antecedentes, cidadania e nacionalidade. A confiabilidade dos desenvolvedores também pode incluir uma revisão e análise da propriedade da empresa e de quaisquer relacionamentos que a empresa tenha com entidades que possam afetar a qualidade / confiabilidade dos sistemas, componentes ou serviços que estão sendo desenvolvidos.  
  
**Melhorias do Controle:**

### SA-21(1): Triagem de Desenvolvedores | Validação da Triagem

A organização exige que o desenvolvedor do sistema de informações, componente do sistema ou serviço do sistema de informações execute [Atribuição: ações definidas pela organização] para garantir que as autorizações de acesso necessárias e os critérios de triagem sejam atendidos.  
Guia Adicional: A satisfação das autorizações de acesso necessárias e dos critérios de triagem de pessoal inclui, por exemplo, fornecer uma lista de todos os indivíduos autorizados a executar atividades de desenvolvimento no sistema de informações, componente do sistema ou serviço do sistema de informações selecionado, para que as organizações possam validar que o desenvolvedor satisfez os requisitos necessários requisitos de autorização e triagem.

## SA-22: Componentes do Sistema Não Suportados (P0)

**Descrição do Controle:**A organização:  
  
a. Substitui os componentes do sistema de informações quando o suporte para os componentes não estiver mais disponível do desenvolvedor, fornecedor ou fabricante; e  
  
b. Fornece justificativa e aprovação de documentos para o uso contínuo de componentes do sistema não suportados, necessários para satisfazer as necessidades da missão / negócios.  
  
**Guia Adicional:**O suporte aos componentes do sistema de informações inclui, por exemplo, patches de software, atualizações de firmware, peças de reposição e contratos de manutenção. Componentes não suportados (por exemplo, quando os fornecedores não estão mais fornecendo patches críticos de software), oferecem uma oportunidade substancial para os adversários explorarem novas fraquezas descobertas nos componentes atualmente instalados. Exceções à substituição de componentes de sistema não suportados podem incluir, por exemplo, sistemas que fornecem capacidade crítica de missão / negócios onde tecnologias mais recentes não estão disponíveis ou onde os sistemas estão tão isolados que a instalação de componentes de substituição não é uma opção.  
  
**Melhorias do Controle:**

### SA-22(1): Componentes do Sistema Não Suportados | Fontes Alternativas para Apoio Contínuo

A organização fornece [Seleção (um ou mais): suporte interno; [Atribuição: suporte definido pela organização de provedores externos]] para componentes não suportados do sistema de informações.  
Guia Adicional: Esse aprimoramento de controle aborda a necessidade de fornecer suporte contínuo aos componentes selecionados do sistema de informações que não são mais suportados pelos desenvolvedores, fornecedores ou fabricantes originais quando esses componentes permanecem essenciais para as operações da missão / negócios. As organizações podem estabelecer suporte interno, por exemplo, desenvolvendo patches personalizados para componentes críticos de software ou proteger os serviços de provedores externos que, por meio de relacionamentos contratuais, fornecem suporte contínuo aos componentes não suportados designados. Tais relações contratuais podem incluir, por exemplo, fornecedores de valor agregado do Software Open Source.