NORMA
BRASILEIRA

ABNT NBR ISO/IEC 27002

Terceira edição
05.10.2022

Segurança da informação, segurança cibernética e proteção à privacidade — Controles de segurança da informação

Information security, cybersecurity and privacy protection — Information security controls

ICS 35.040

ISBN 978-85-07-09276-6

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS

Número de referência
ABNT NBR ISO/IEC 27002:2022
191 páginas

Documento impresso em 27/06/2023 22:08:50, de uso exclusivo de UNIVERSIDADE FEDERAL DO CEARÁ

ABNT
Av. Treze de Maio, 13 - 28º andar
20031-901 - Rio de Janeiro - RJ
Tel.: + 55 21 3974-2300
Fax: + 55 21 3974-2346
abnt@abnt.org.br
www.abnt.org.br

Sumário

Página

Tabelas

Prefácio Nacional

A Associação Brasileira de Normas Técnicas (ABNT) é o Foro Nacional de Normalização. As Normas Brasileiras, cujo conteúdo é de responsabilidade dos Comitês Brasileiros (ABNT/CB), dos Organismos de Normalização Setorial (ABNT/ONS) e das Comissões de Estudo Especiais (ABNT/CEE), são elaboradas por Comissões de Estudo (CE), formadas pelas partes interessadas no tema objeto da normalização.

Os Documentos Técnicos internacionais adotados são elaborados conforme as regras da ABNT Diretiva 3.

A ABNT chama a atenção para que, apesar de ter sido solicitada manifestação sobre eventuais direitos de patentes durante a Consulta Nacional, estes podem ocorrer e devem ser comunicados à ABNT a qualquer momento (Lei nº 9.279, de 14 de maio de 1996).

Os Documentos Técnicos ABNT, assim como as Normas Internacionais (ISO e IEC), são voluntários e não incluem requisitos contratuais, legais ou estatutários. Os Documentos Técnicos ABNT não substituem Leis, Decretos ou Regulamentos, aos quais os usuários devem atender, tendo precedência sobre qualquer Documento Técnico ABNT.

Ressalta-se que os Documentos Técnicos ABNT podem ser objeto de citação em Regulamentos Técnicos. Nestes casos, os órgãos responsáveis pelos Regulamentos Técnicos podem determinar as datas para exigência dos requisitos de quaisquer Documentos Técnicos ABNT.

A ABNT NBR ISO/IEC 27002 foi elaborada no Comitê Brasileiro de Tecnologias da Informação e Transformação Digital (ABNT/CB-021), pela Comissão de Estudo de Segurança da Informação, Segurança Cibernética e Proteção da Privacidade (CE-021:004.027). O Projeto de Revisão circulou em Consulta Nacional conforme Edital nº 07, de 19.07.2022 a 17.08.2022.

A ABNT NBR ISO/IEC 27002 é uma adoção idêntica, em conteúdo técnico, estrutura e redação, à ISO/IEC 27002:2022, que foi elaborada pelo *Joint Technical Committee Information Technology* (ISO/JTC 1), *Subcommittee Information security, Cybersecurity and Privacy Protection* (SC 27).

A ABNT NBR ISO/IEC 27002:2022 cancela e substitui a ABNT NBR ISO/IEC 27002:2012, a qual foi tecnicamente revisada.

A ABNT NBR ISO/IEC 27002:2022 relaciona a seguir os termos que foram mantidos integral ou parcialmente na língua inglesa, com a sua descrição, por não possuírem tradução equivalente para a língua portuguesa, e por serem de uso comum no âmbito da segurança da informação, segurança cibernética e proteção da privacidade.

— *Anti-malware:* sistema de proteção contra softwares maliciosos (*"malware"*)

— Ataques de *scripting* entre *sites*: tipo de ataque de injeção de código ou *script* malicioso em *sites*

— *Backup*: cópia de segurança

— *Botnet*: rede de computadores infectados controlados remotamente para realizar ataques.

— *Buffer overflow*: qualquer técnica de ataque que explore uma vulnerabilidade de *software* ou *hardware* de computador em que não é verificada a ultrapassagem dos limites de uma área de armazenamento quando os dados são gravados nessa área.

- *Feeds* de vídeo: transmissão contínua de dados em formato de vídeo.
- *Firewall*: dispositivo ou sistema que controla o tráfego de entrada e saída de informações entre as redes conectadas em suas interfaces.
- *Gateway*: dispositivo ou sistema que permite interligar redes distintas. Por exemplo, conectar à rede interna da organização à *Internet*.
- *Hardening* do sistema: processo de aplicação de configurações de segurança e outras medidas técnicas que tornam o sistema mais seguro.
- *Hashing*: processo de geração de um código de tamanho fixo a partir da aplicação de uma fórmula matemática (função *hash*) a um dado de tamanho variável. É usado, por exemplo, no controle de senhas, permitindo que se possa validar uma senha sem a necessidade de armazená-la (o que fica na base de dados é o resultado da função *hash*).
- *Honeypots*: armadilha destinada a atrair intrusos que tentam invadir um sistema
- *Wipe*: método que visa destruir completamente todos os dados que residem em uma unidade de disco rígido ou outra mídia digital, usando “0 e 1” para sobrescrever os dados em todos os setores do dispositivo, em um processo irreversível.
- *Logging*: processo de registro sistemático de informações sobre eventos que ocorreram em sistemas e recursos de TIC.
- *Malware*: termo genérico para se referir a *software* criado com intenção maliciosa, projetado para infiltrar um sistema computacional com a intenção de roubar dados ou danificar aplicativos ou o sistema operacional
- *Patches*: atualizações e correções efetuadas em um programa, sistema ou equipamento existente, com intenção de corrigir uma vulnerabilidade específica.
- Parâmetros de *host*: parâmetros de configuração e customização de ferramentas, aplicativos ou sistemas operacionais em um determinado equipamento (chamado de “*host*”).
- *Phishing*: técnica de ataque cibernético utilizada para tentar adquirir dados confidenciais dos usuários, como números e senhas de contas bancárias, por meio de uma solicitação fraudulenta por mensagens de *e-mail* ou em sites da *web*, na qual o perpetrador se disfarça de empresa
- *Bollards*: barreiras físicas que impedem o acesso a determinadas áreas que necessitam desse tipo de proteção.
- Programas de recompensa por *bugs*: programa que autoriza terceiros a realizarem avaliações de segurança em seus ativos tecnológicos, com o intuito de identificar falhas e, em troca, oferecem recompensas.
- *Refactoring*: processo de melhoria no sistema de *software*, de forma que sua estrutura interna seja aprimorada, sem que o comportamento ou funcionalidades do sistema sejam alterados.
- *Salt function*: valor único adicionado a uma senha, normalmente em seu final, para alterar e, consequentemente, proteger o resultado do *hash* contra-ataques de força bruta que visem descobrir as senhas armazenadas em uma base.

— *Scripts*: conjunto de instruções, em geral escritos para automatizar alguma atividade. São também conhecidos como linguagem de *scripting* ou linguagem de extensão.

— *Single Sign On* (SSO): processo de autenticação que permite o acesso a diversos sistemas com o uso das mesmas credenciais de acesso.

— *Slots* de cartão SD: dispositivos que permitem a leitura e escrita em cartões do tipo SD (*Secure Digital*), muito comuns em dispositivos portáteis.

O Escopo da ABNT NBR ISO/IEC 27002 em inglês é o seguinte:

Scope

This document provides a reference set of generic information security controls including implementation guidance. This document is designed to be used by organizations:

a) within the context of an information security management systems (ISMS) based on ABNT NBR ISO/IEC 27001;

b) for implementing information security controls based on internationally recognized best practices;

c) for developing organization-specific information security management guidelines.

Introdução

0.1 Histórico e contexto

Este documento é projetado para organizações de todos os tipos e tamanhos. É para ser usado como referência para determinar e implementar controles para tratamento de riscos de segurança da informação em um sistema de gestão de segurança da informação (SGSI) baseado na ABNT NBR ISO/IEC 27001. Também pode ser usado como um documento de orientação para organizações determinando e implementando controles de segurança da informação comumente aceitos. Além disso, este documento é destinado a ser utilizado no desenvolvimento de diretrizes de gestão de segurança da informação específicas para a indústria e a organização, considerando seu ambiente específico de riscos de segurança da informação. Controles organizacionais ou específicos do ambiente que não sejam os incluídos neste documento podem ser determinados através do processo de avaliação de riscos, conforme necessário.

Organizações de todos os tipos e tamanhos (incluindo setor público e privado, comercial e sem fins lucrativos) criam, coletam, tratam, armazenam, transmitem e descartam informações de diversas formas, incluindo eletrônica, física e verbal (por exemplo, conversas e apresentações).

O valor da informação vai além das palavras, escritas, números e imagens: conhecimentos, conceitos, ideias e marcas são exemplos de formas intangíveis de informação. Em um mundo interconectado, informações e outros ativos associados merecem ou requerem proteção contra várias fontes de risco, sejam naturais, acidentais ou deliberadas.

A segurança da informação é alcançada por meio da implementação de um conjunto adequado de controles, incluindo políticas, regras, processos, procedimentos, estruturas organizacionais e funções de *software* e *hardware*. Para atender aos seus objetivos específicos de segurança e negócios, convém que a organização defina, implemente, monitore, analise criticamente e aprimore esses controles quando necessário. Um SGSI como o especificado na ABNT NBR ISO/IEC 27001 tem uma visão holística e coordenada dos riscos de segurança da informação da organização, a fim de determinar e implementar um conjunto abrangente de controles de segurança da informação na estrutura geral de um sistema de gestão coerente.

Muitos sistemas de informação, incluindo de gestão e operações, não foram projetados para serem seguros em termos de um SGSI conforme especificado na ABNT NBR ISO/IEC 27001 e neste documento. O nível de segurança que só pode ser alcançado por meio de medidas tecnológicas é limitado e convém que seja apoiado por atividades de gestão e processos organizacionais adequados. Identificar quais controles convém que estejam implementados requer um planejamento cuidadoso e atenção aos detalhes durante a realização do tratamento de riscos.

Um SGSI bem-sucedido requer o apoio de todo o pessoal da organização. Também pode requerer a participação de outras partes interessadas, como acionistas ou fornecedores. Assessoria de especialistas no assunto também pode ser necessária.

Um sistema de gestão da segurança da informação apropriado, adequado e eficaz fornece garantia à direção da organização e a outras partes interessadas de que suas informações e outros ativos associados estão mantidos razoavelmente seguros e protegidos contra ameaças e danos, permitindo assim que a organização atinja os objetivos de negócios declarados.

0.2 Requisitos de segurança da informação

É essencial que a organização determine seus requisitos de segurança da informação. Existem três principais fontes de requisitos de segurança da informação:

a) a avaliação de riscos da organização, considerando a estratégia e os objetivos globais de negócios da organização. Isso pode ser facilitado ou apoiado por meio de um processo de avaliação de riscos específico de segurança da informação. Convém que isso resulte na determinação dos controles necessários para assegurar que o risco residual à organização atenda aos seus critérios de aceitação de riscos;

b) os requisitos legais, estatutários, regulamentares e contratuais que uma organização e suas partes interessadas (parceiros comerciais, prestadores de serviços etc.) têm que cumprir e seu ambiente sociocultural;

c) o conjunto de princípios, objetivos e requisitos de negócios para todas as etapas do ciclo de vida de informações que uma organização desenvolveu para apoiar suas operações.

0.3 Controles

Um controle é definido como uma medida que modifica ou mantém o risco. Alguns dos controles deste documento são controles que modificam o risco, enquanto outros mantêm o risco. Uma política de segurança da informação, por exemplo, só pode manter o risco, enquanto o cumprimento da política de segurança da informação pode modificar o risco. Além disso, alguns controles descrevem a mesma medida genérica em diferentes contextos de riscos. Este documento fornece uma mistura genérica de controles organizacionais, de pessoas e de segurança da informação física e tecnológica derivados de melhores práticas reconhecidas internacionalmente.

0.4 Determinando controles

A determinação dos controles é dependente das decisões da organização após um processo de avaliação de riscos, com um escopo claramente definido. Convém que as decisões relacionadas aos riscos identificados se baseiem nos critérios de aceitação de riscos, nas opções de tratamento de riscos e na abordagem de gestão de riscos aplicada pela organização. Convém que a determinação dos controles também considere todas as legislações e regulamentações nacionais e internacionais relevantes. A determinação do controle também depende da forma como os controles interagem entre si para fornecer defesa em profundidade.

A organização pode projetar controles conforme necessário ou identificá-los de qualquer fonte. Ao especificar estes controles, convém que as organizações considerem os recursos e investimentos necessários para implementar e operar um controle comparado com o valor de negócios realizado. Ver o ISO/IEC TR 27016 para orientação sobre as decisões relativas ao investimento em um SGSI e as consequências econômicas dessas decisões no contexto de requisitos concorrentes para os recursos.

Convém que exista um equilíbrio entre os recursos alocados para a implementação de controles e o potencial impacto nos negócios resultantes de incidentes de segurança na ausência desses controles. Convém que os resultados de uma avaliação de riscos ajude a orientar e determinar as ações de gestão adequadas, as prioridades para gerenciar riscos de segurança da informação e para implementar os controles determinados para proteger contra esses riscos.

Alguns dos controles deste documento podem ser considerados como princípios orientadores para a gestão da segurança da informação e como aplicáveis para a maioria das organizações. Mais

informações sobre a determinação de controles e outras opções de tratamento de risco podem ser encontradas na ABNT NBR ISO/IEC 27005.

0.5 Desenvolvendo diretrizes específicas da organização

Este documento pode ser considerado como um ponto de partida para o desenvolvimento de diretrizes específicas da organização. Nem todos os controles e orientações deste documento podem ser aplicáveis a todas as organizações. Controles e diretrizes adicionais não incluídas neste documento também podem ser necessários para atender às necessidades específicas da organização e aos riscos identificados. Quando documentos são elaborados contendo diretrizes ou controles adicionais, pode ser útil incluir referências cruzadas às seções deste documento para referência futura.

0.6 Considerações do ciclo de vida

A informação tem um ciclo de vida natural, da criação ao descarte. O valor e os riscos para as informações podem variar ao longo deste ciclo de vida (por exemplo, divulgação indevida ou roubo dos resultados financeiros de uma empresa não é significativa depois de serem publicadas, mas a integridade permanece crítica) portanto, a segurança da informação permanece importante em alguma medida em todas as etapas.

Os sistemas de informação e outros ativos relevantes para a segurança da informação possuem ciclos de vida dentro dos quais são concebidos, especificados, projetados, desenvolvidos, testados, implementados, usados, mantidos e eventualmente retirados do serviço e descartados. Convém que a segurança da informação seja considerada em todas as etapas. Novos projetos de desenvolvimento de sistemas e mudanças nos sistemas existentes oferecem oportunidades para melhorar os controles de segurança, considerando os riscos e lições aprendidas com os incidentes.

0.7 Normas relacionadas

Embora este documento ofereça orientações sobre uma ampla gama de controles de segurança da informação que são comumente aplicados em muitas organizações diferentes, outros documentos da família ISO/IEC 27000 fornecem orientações ou requisitos complementares sobre outros aspectos do processo global de gestão da segurança da informação.

Ver a ISO/IEC 27000 para uma introdução geral ao SGSI e à família de documentos. A ISO/IEC 27000 fornece um glossário, definindo a maioria dos termos utilizados em toda a família de documentos ISO/IEC 27000, e descreve o escopo e objetivos para cada membro da família.

Existem normas setoriais específicas que têm controles adicionais que visam abordar áreas específicas (por exemplo, ABNT NBR ISO/IEC 27017, para serviços em nuvem, ABNT NBR ISO/IEC 27701, para privacidade, ISO/IEC 27019, para energia, ISO/IEC 27011, para organizações de telecomunicações e ISO 27799, para saúde). Estas normas estão incluídas na Bibliografia e algumas delas são referenciadas nas seções de orientação e outras informações nas Seções 5 a 8.

Documento impresso em 27/06/2023 22:08:50, de uso exclusivo de UNIVERSIDADE FEDERAL DO CEARÁ

Segurança da informação, segurança cibernética e proteção à privacidade — Controles de segurança da informação

1 Escopo

Este documento fornece um conjunto de referência de controles genéricos de segurança da informação, incluindo orientação para implementação. Este documento foi projetado para ser usado pelas organizações:

a) no contexto de um sistema de gestão de segurança da informação (SGSI) baseado na ABNT NBR ISO/IEC 27001;

b) para a implementação de controles de segurança da informação com base em melhores práticas reconhecidas internacionalmente;

c) para o desenvolvimento de diretrizes específicas de gestão de segurança da informação da organização.

2 Referências normativas

Não há referências normativas neste documento.

3 Termos e definições

Para os efeitos deste documento, aplicam-se os seguintes termos e definições.

3.1 Termos e definições

Para efeitos deste documento, aplicam-se os seguintes termos e definições.

O ISO e a IEC mantêm bases de dados terminológicos para uso na normalização nos seguintes endereços:

— ISO *Online browsing plataforma:* disponível em http://www.iso.org.obp

— IEC *Electropedia:* disponível em http://www.electropedia.org/

3.1.1
controle de acesso
significa assegurar que o acesso físico e lógico aos *ativos* (3.1.2) seja autorizado e restrito com base em requisitos de negócio e de segurança da informação

3.1.2
ativo
qualquer coisa que tenha valor para a organização

Nota 1 de entrada: No contexto da segurança da informação, dois tipos de ativos podem ser distinguidos:

— os ativos primários:

  — informação;

  — *processos* (3.1.27) de negócios e atividades;

— os ativos de suporte (dos quais os ativos primários dependem) de todos os tipos, por exemplo:

  — *hardware;*

  — *software;*

  — rede;

  — *pessoal* (3.1.20);

  — local;

  — estrutura da organização.

3.1.3
ataque
tentativa não autorizada, bem-sucedida ou malsucedida, de destruir, alterar, desabilitar, obter acesso a um *ativo* (3.1.2) ou qualquer tentativa de expor, roubar ou fazer uso não autorizado de um *ativo* (3.1.2)

3.1.4
autenticação
provisão de garantia de que uma característica alegada de uma *entidade* (3.1.11) está correta

3.1.5
autenticidade
propriedade que uma *entidade* (3.1.11) é o que ela alega ser

3.1.6
cadeia de custódia
demonstrável posse, movimento, manuseio e localização de material de um ponto no tempo até outro

Nota 1 de entrada: Material inclui informações e outros *ativos* (3.1.2) associados no contexto da ABNT NBR ISO/IEC 27002.

[FONTE: ISO/IEC 27050-1:2019, 3.1, modificada – “Nota 1 de entrada” adicionada]

3.1.7
informações confidenciais
informações que não se destinam a ser disponibilizadas ou divulgadas a indivíduos, *entidades* (3.1.11) ou *processos* (3.1.27) não autorizados

3.1.8
controle
medida que mantém e/ou modifica o risco

Nota 1 de entrada: Controles incluem, mas não estão limitados a, qualquer *processo* (3.1.27), *política* (3.1.24), dispositivo, prática ou outras condições e/ou ações que mantêm e/ou modificam o risco.

Nota 2 de entrada: Controles podem nem sempre exercer o efeito modificador pretendido ou presumido.

[FONTE: ABNT NBR ISO 31000:2018, 3.8]

3.1.9
disrupção
incidente, seja previsto ou imprevisto, que causa um desvio, não planejado e negativo da expectativa de entrega de produtos e serviços de acordo com os objetivos da organização

[FONTE: ABNT NBR ISO 22301:2020, 3.10]

3.1.10
dispositivo *endpoint*
dispositivo de *hardware* de tecnologia da informação e comunicação (TIC) conectado à rede

Nota 1 de entrada: Dispositivo *endpoint* pode se referir a computadores *desktop*, *laptops*, *smartphones*, *tablets*, *thin clients*, impressoras ou outros *hardwares* especializados, incluindo medidores inteligentes e dispositivos de *Internet* das Coisas (IoT).

3.1.11
entidade
item relevante para o propósito de operação de um domínio que tem existência reconhecidamente distinta

Nota 1 de entrada: Uma entidade pode ter uma personificação física ou lógica.

EXEMPLO Uma pessoa, uma organização, um dispositivo, um grupo desses itens, um assinante humano de um serviço de telecomunicações, um cartão SIM, um passaporte, um cartão de interface de rede, uma aplicação de *software*, um serviço ou um *website*.

[FONTE: ISO/IEC 24760-1:2019, 3.1.1]

3.1.12
ambiente de tratamento de informações
qualquer sistema de tratamento de informações, serviço ou infraestrutura, ou a localização física que o abriga

[FONTE: ISO/IEC 27000:2018, 3.27, modificado – "*facilities*" foi substituído por ambiente.]

3.1.13
violação de segurança da informação
comprometimento de segurança da informação que leva à destruição indesejada, perda, alteração, divulgação de, ou acesso a, informações protegidas transmitidas, armazenadas ou tratadas de diversas formas

3.1.14
evento de segurança da informação
ocorrência indicando uma possível *violação de segurança da informação* (3.1.13) ou falha de *controles* (3.1.8)

[FONTE: ISO/IEC 27035-1:2016, 3.3]

NOTA BRASILEIRA A informação de substituição do termo "*breach of information security*" por "*information security breach*" foi excluída tendo em vista que não é aplicável na língua portuguesa.

3.1.15
incidente de segurança da informação
um ou múltiplos *eventos de segurança da informação* (3.1.14) relacionados e identificados que podem prejudicar os *ativos* (3.1.2) da organização ou comprometer suas operações

[FONTE: ISO/IEC 27035-1:2016, 3.4]

3.1.16
gestão de incidentes de segurança da informação
exercício de uma abordagem consistente e eficaz para o manuseio de *incidentes de segurança da informação* (3.1.15)

[FONTE: ISO/IEC 27035-1:2016, 3.5]

3.1.17
sistema de informação
conjunto de aplicações, serviços, *ativos* (3.1.2) de tecnologia da informação ou outros componentes de manuseio de informações

[FONTE: ISO/IEC 27000:2018, 3.35]

3.1.18
parte interessada
stakeholder
pessoa ou organização interessada que pode afetar, ser afetada ou perceber-se afetada por, uma decisão ou atividade

[FONTE: ISO/IEC 27000:2018, 3.37]

3.1.19
não repúdio
capacidade de comprovar a ocorrência de um evento ou ação declarada e suas *entidades* (3.1.11) originárias

3.1.20
pessoal
pessoas que executam trabalho sob a direção da organização

Nota 1 de entrada: O conceito de pessoal inclui os membros da organização, como o órgão diretivo, a Alta Direção, os funcionários, a equipe de temporários, os fornecedores e os voluntários.

3.1.21
dados pessoais
DP
qualquer informação que (a) possa ser usada para identificar a pessoa natural à qual tal informação se relaciona ou (b) é ou pode ser direta ou indiretamente vinculada a uma pessoa natural

Nota 1 de entrada: A “pessoa natural” na definição é o *titular de DP* (3.1.22). Para determinar se um titular de DP é identificável, convém que sejam considerados todos os meios que possam ser razoavelmente usados pela parte interessada privacidade, detentora dos dados, ou por qualquer outra parte, para identificar a pessoa natural.

[FONTE: ABNT NBR ISO/IEC 29100:2020, 2.7]

3.1.22
titular de DP
pessoa natural a quem se referem os *dados pessoais (DP)* (3.1.21)

Nota 1 de entrada: Dependendo da jurisdição e da legislação específica de proteção de dados e privacidade, o sinônimo de “sujeito dos dados” pode ser usado em vez do termo “titular de DP”.

[FONTE: ABNT NBR ISO/IEC 29100:2020, 2.9]

3.1.23
operador de DP
parte interessada na privacidade, que faz o tratamento dos dados pessoais (DP) (3.1.21) em benefício e de acordo com as instruções de um controlador de DP

[FONTE: ABNT NBR ISO/IEC 29100:2020, 2.10]

3.1.24
política
intenções e direção de uma organização, expressa formalmente por sua Alta Direção

[FONTE: ISO/IEC 27000:2018, 3.53]

3.1.25
análise de impacto de privacidade
PIA
processo (3.1.27) geral de identificação, análise, avaliação, consultoria, comunicação e planejamento do tratamento de potenciais impactos à privacidade com relação ao tratamento de DP (3.1.21), contidos em uma estrutura mais ampla de gestão de riscos da organização

[FONTE: ABNT NBR ISO/IEC 29134:2020, 3.7, modificado – Nota 1 de entrada removida.]

3.1.26
procedimento
modo especificado de realizar uma atividade ou um *processo* (3.1.27)

[FONTE: ISO 30000:2009, 3.12]

3.1.27
processo
conjunto de atividades inter-relacionadas ou interativas que utilizam entradas para entregar um resultado pretendido

[FONTE: ABNT NBR ISO 9000:2015, 3.4.1, modificado – Notas de entrada removidas.]

3.1.28
registro
informações criadas, recebidas e mantidas como evidência e como um *ativo* (3.1.2) por uma organização ou pessoa, em busca de obrigações legais ou na transação de negócios

Nota 1 de entrada: As obrigações legais neste contexto incluem todos os requisitos legais, estatutários, regulamentares e contratuais.

[FONTE: ISO 15489-1:2016, 3.14, modificado – “Nota 1 de entrada” adicionada.]

3.1.29
ponto objetivado de recuperação
RPO
ponto em uma linha de tempo em que os dados sejam recuperados após a ocorrência de uma disrupção (3.1.9)

[FONTE: ISO/IEC 27031:2011, 3.12, modificado – "devem ser (*must*)" substituído por "sejam (*are to be*)".]

3.1.30
tempo objetivado de recuperação
RTO
período de tempo dentro do qual os níveis mínimos de serviços e/ou produtos e os sistemas de suporte, aplicações ou funções sejam recuperados após a ocorrência de uma *disrupção* (3.1.9)

[FONTE: ISO/IEC 27031:2011, 3.13, modificado – "devem ser (*must*)" substituído por "sejam (*are to be*)".]

3.1.31
confiabilidade
propriedade de comportamento e resultados pretendidos consistentes

3.1.32
regra
princípio ou instrução aceita que declara as expectativas da organização sobre o que é necessário que seja feito, o que é permitido ou não permitido

Nota 1 de entrada: Regras podem ser expressas formalmente em *políticas específicas por tema* (3.1.35) e em outros tipos de documentos.

3.1.33
informações sensíveis
informações que precisam ser protegidas contra indisponibilidade, acesso, modificação ou divulgação pública não autorizada devido a potenciais efeitos adversos em um indivíduo, organização, segurança nacional ou segurança pública

3.1.34
ameaça
causa potencial de um incidente indesejado, que pode resultar em danos a um sistema ou organização

[FONTE: ISO/IEC 27000:2018, 3.74]

3.1.35
política específica por tema
intenções e direção sobre um assunto ou tema específico, como formalmente expressos pelo nível apropriado de gestão

Nota 1 de entrada: As políticas específicas por tema podem expressar formalmente *regras* (3.1.32) ou normas da organização.

Nota 2 de entrada: Algumas organizações usam outros termos para essas políticas específicas por tema.

Nota 3 de entrada: As políticas específicas por tema neste documento estão relacionadas à segurança da informação.

EXEMPLO A política específica para o controle de *acesso* (3.1.1), política específica de mesa e tela limpa.

3.1.36
usuário
partes interessadas (3.1.18) com acesso aos *sistemas de informação* (3.1.17) da organização

EXEMPLO *Pessoal* (3.1.20), clientes, fornecedores.

3.1.37
dispositivo *endpoint* do usuário
dispositivo endpoint (3.1.10) usado pelos usuários para acessar serviços de tratamento de informações

Nota 1 de entrada: O dispositivo *endpoint* do usuário pode se referir a computadores *desktop*, *laptops*, *smartphones*, *tablets*, *thin clients* etc.

3.1.38
vulnerabilidade
fraqueza de um *ativo* (3.1.2) ou *controle* (3.1.8) que pode ser explorado por uma ou mais *ameaças* (3.1.34)

[FONTE: ISO/IEC 27000:2018, 3.77]

3.2 Termos abreviados

ABAC	controle de acesso baseado em atributos (*attribute-based access control*)
ACL	lista de controle de acesso (*access control list*)
BIA	análise de impacto nos negócios (*business impact analysis*)
BYOD	traga seu próprio dispositivo (*bring your own device*)
CAPTCHA	teste de Turing (*completely automated public Turing test to tell computers and humans apart*)
CPU	unidade central de processamento (*central processing unit*)
DAC	controle de acesso discricionário (*discretionary access control*)
DNS	sistema de nome de domínio (*domain name system*)
GPS	sistema de posicionamento global (*global positioning system*)
IAM	gestão de identidade e acesso (*identity and access management*)
TIC	tecnologia da informação e comunicação (*information and communication technology*)
ID	identificador (*identifier*)
IDE	ambiente de desenvolvimento integrado (*integrated development environment*)
IDS	sistema de detecção de intrusão (*intrusion detection system*)
IoT	*internet* das coisas (*internet of things*)
IP	protocolo de internet (*internet protocol*)
IPS	sistema de prevenção de intrusão (*intrusion prevention system*)

TI	tecnologia da informação (*information technology*)
SGSI	sistema de gestão de segurança da informação (*information security management system*)
MAC	controle de acesso obrigatório (*mandatory access control*)
NTP	protocolo de tempo de rede (*network time protocol*)
PIA	análise de impacto de privacidade (*privacy impact assessment*)
DP	dados pessoais (*personally identifiable information*)
PIN	número de identificação pessoal (*personal identification number*)
PKI	infraestrutura de chave pública (*public key infrastructure*)
PTP	protocolo de tempo de precisão (*precision time protocol*)
RBAC	controle de acesso baseado em papel (*role-based access control*)
RPO	ponto objetivado de recuperação (*recovery point objective*)
RTO	tempo objetivado de recuperação (*recovery time objective*)
SAST	teste de segurança de aplicações estáticas (static application security testing)
SD	digital segura (*secure digital*)
SDN	redes definidas por *software* (*software-defined networking*)
SD-WAN	rede WAN definida por *software* (*software-defined wide area networking*)
SIEM	gerenciamento de eventos de segurança da informação (*security information and event management*)
SMS	serviço de mensagem curta (*short message service*)
SQL	linguagem de consulta estruturada (*structured query language*)
SSO	identificação única (*single sign-on*)
SWID	identificação de *software* (*software identification*)
UEBA	análise de comportamento do usuário e da entidade (*user and entity behaviour analytics*)
UPS	fonte de energia ininterrupta (*uninterruptible power supply*)
URL	localizador de recursos uniforme (*uniform resource locator*)
USB	barramento serial universal (*universal serial bus*)
VM	máquina virtual (*virtual machine*)
VPN	rede virtual privada (*virtual private network*)
WiFi	rede sem fio (*wireless fidelity*)

4 Estrutura deste documento

4.1 Seções

Este documento está estruturado da seguinte forma:

a) Controles organizacionais (Seção 5).

b) Controles de pessoas (Seção 6).

c) Controles físicos (Seção 7).

d) Controles tecnológicos (Seção 8).

Existem dois anexos informativos:

— Anexo A –Uso de atributos

— Anexo B – Correspondência com a ABNT NBR ISO/IEC 27002:2013

O Anexo A explica como uma organização pode usar atributos (ver 4.2) para criar suas próprias visões com base nos atributos de controle definidos neste documento ou de sua própria criação.

O Anexo B mostra a correspondência entre os controles nesta edição da ABNT NBR ISO/IEC 27002 e da edição anterior de 2013.

4.2 Temas e atributos

A categorização dos controles dados nas Seções 5 a 8 é referida como temas. Os controles são categorizados como:

a) pessoas, se eles dizem respeito a pessoas individuais;

b) físico, se eles dizem respeito a objetos físicos;

c) tecnológico, se eles dizem respeito à tecnologia;

d) caso contrário, eles são categorizados como organizacionais.

A organização pode usar atributos para criar diferentes visões que são categorizações diferentes dos controles, vistas de uma perspectiva diferente dos temas. Atributos podem ser usados para filtrar, classificar ou apresentar controles em diferentes pontos de vista para diferentes públicos. O Anexo A explica como isso pode ser alcançado e fornece um exemplo de uma visão.

Por exemplo, cada controle neste documento foi associado a cinco atributos com valores de atributo correspondentes (precedidos por “#” para torná-los pesquisáveis), da seguinte forma:

a) Tipo de controle

   O tipo de controle é um atributo para visualizar controles sob a perspectiva de quando e como o controle modifica o risco em relação à ocorrência de um incidente de segurança da informação. Os valores de atributo consistem em Preventivo (o controle que se destina a evitar a ocorrência de um incidente de segurança da informação), Detectivo (o controle age quando ocorre um incidente

de segurança da informação) e Corretivo (o controle age após um incidente de segurança da informação ocorrer).

b) Propriedades de segurança da informação

As propriedades de segurança da informação são um atributo para visualizar controles na perspectiva de qual característica das informações o controle contribuirá para a preservação. Os valores dos atributos consistem em Confidencialidade, Integridade e Disponibilidade.

c) Conceitos de segurança cibernética

Os conceitos de segurança cibernética são um atributo para visualizar os controles sob a perspectiva da associação de controles aos conceitos de segurança cibernética definidos no quadro de segurança cibernética descrito no ISO/IEC TS 27110. Os valores dos atributos consistem em Identificar, Proteger, Detectar, Responder e Recuperar.

d) Capacidades operacionais

As capacidades operacionais são um atributo para visualizar controles da perspectiva do praticante sobre os recursos de segurança da informação. Os valores de atributos consistem em Governança, Gestão_de_ativos, Proteção_da_informação, Segurança_em_recursos_humanos, Segurança_física, Segurança_de_sistemas_e_redes, Segurança_de_aplicações, Configuração_segura, Gestão_de_identidade_e_acesso, Gestão_de_ameaças_e_vulnerabilidades, Continuidade, Segurança_do_relacionamento_na_cadeia_de_suprimentos, Legal_e_*compliance*, Gestão_de_eventos_de_segurança_da_informação e Garantia_de_segurança_da_informação.

e) Domínios de segurança

Os domínios de segurança são um atributo para visualizar controles na perspectiva de quatro domínios de segurança da informação: “Governança_e_Ecossistema” inclui “Governança do Sistema de Segurança da Informação e Gestão de Riscos” e “Gestão de segurança cibernética do ecossistema” (incluindo partes interessadas internas e externas); “Proteção” inclui “Arquitetura de Segurança de TI”, “Administração de Segurança de TI”, “Gestão de identidade e acesso”, “Manutenção de Segurança de TI” e “Segurança física e ambiental”; “Defesa” inclui “Detectar” e “Gestão de Incidente de segurança computacional”; Resiliência inclui “Operações de continuidade” e “Gestão de crises”. Os valores de atributos consistem em Governança_e_Ecossistema, Proteção, Defesa e Resiliência.

Os atributos dados neste documento são selecionados porque são considerados genéricos o suficiente para serem usados por diferentes tipos de organizações. As organizações podem optar por ignorar um ou mais dos atributos dados neste documento. Eles também podem criar atributos próprios (com os valores de atributo correspondentes) para criar suas próprias visões organizacionais. A Seção A.2 inclui exemplos destes atributos.

4.3 *Layout* dos controles

O *layout* para cada controle contém o seguinte:

— **Título do controle**: Nome curto do controle;

— **Tabela de atributos**: Uma tabela mostra o(s) valor(es) de cada atributo para o controle dado;

— **Controle**: Qual é o controle;

— **Propósito**: Por que convém que o controle seja implementado;

— **Orientação**: Como convém que o controle seja implementado;

— **Outras informações**: Texto explicativo ou referências a outros documentos relacionados.

Subtítulos são usados no texto de orientação para alguns controles para auxiliar a legibilidade onde a orientação é longa e aborda vários tópicos. Tais títulos não são necessariamente usados em todos os textos de orientação. Subtítulos são sublinhados.

5 Controles organizacionais

5.1 Políticas de segurança da informação

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Identificar	#Governança	#Governança_e_Ecossistema #Resiliência

Controle

Convém que a política de segurança da informação e as políticas específicas por tema sejam definidas, aprovadas pela direção, publicadas, comunicadas e reconhecidas pelo pessoal pertinente e partes interessadas pertinentes, e analisadas criticamente em intervalos planejados e se ocorrer mudanças significativas.

Propósito

Assegurar a adequação contínua, suficiência, efetividade da direção de gestão e suporte à segurança da informação de acordo com os requisitos comerciais, legais, estatutários, regulamentares e contratuais.

Orientação

No mais alto nível, convém que a organização defina uma “política de segurança da informação” aprovada pela Alta Direção e que estabeleça a abordagem da organização para gerenciar sua segurança da informação.

Convém que a política de segurança da informação considere os requisitos derivados de:

a) estratégia e requisitos de negócios;

b) regulamentações, legislação e contratos;

c) riscos e ameaças atuais e projetados para a segurança da informação.

Convém que a política de segurança da informação contenha declarações relativas a:

a) definição de segurança da informação;

b) objetivos de segurança da informação ou a estrutura para definir objetivos de segurança da informação;

c) princípios para orientar todas as atividades relacionadas à segurança da informação;

d) comprometimento de satisfazer os requisitos aplicáveis relacionados à segurança da informação;

e) comprometimento com a melhoria contínua do sistema de gestão da segurança da informação;

f) atribuição de responsabilidades para a gestão da segurança da informação para funções definidas;

g) procedimentos para tratamento de isenções e exceções.

Convém que a Alta Direção aprove quaisquer alterações na política de segurança da informação.

Em um nível mais baixo, convém que a política de segurança da informação seja apoiada por políticas específicas por tema, conforme necessário para obrigar ainda mais a implementação de controles de segurança da informação. As políticas específicas por tema são tipicamente estruturadas para atender às necessidades de determinados grupos-alvo dentro de uma organização ou para cobrir determinadas áreas de segurança. Convém que as políticas específicas por tema sejam alinhadas e complementares à política de segurança da informação da organização.

Exemplos destes temas incluem:

a) controle de acesso;

b) segurança física e do ambiente;

c) gestão de ativos;

d) transferência de informações;

e) configuração e manuseio seguros de dispositivos *endpoint* do usuário;

f) segurança de redes;

g) gestão de incidentes de segurança da informação;

h) *backup*;

i) criptografia e gerenciamento de chaves;

j) classificação e tratamentos de informações;

k) gestão de vulnerabilidades técnicas;

l) desenvolvimento seguro.

Convém que a responsabilidade pelo desenvolvimento, análise crítica e aprovação das políticas específicas por tema seja atribuída ao pessoal pertinente com base no seu nível adequado de autoridade e competência técnica. Convém que a análise crítica inclua a avaliação de oportunidades de melhoria da política de segurança da informação da organização e das políticas de específicas por tema e a gestão da segurança da informação em resposta às mudanças no seguinte:

a) estratégia de negócios da organização;

b) ambiente técnico da organização;

c) regulamentos, estatutos, legislação e contratos;

d) riscos à segurança da informação;

e) ambiente atual e projetado de ameaça à segurança da informação;

f) lições aprendidas com eventos e incidentes de segurança da informação.

Convém que a análise crítica da política de segurança da informação e das políticas específicas por tema considere os resultados das análises críticas pela direção e das auditorias. Convém que a análise crítica e atualização de outras políticas relacionadas sejam consideradas quando uma política é alterada para manter a consistência.

Convém que a política de segurança da informação e as políticas específicas por tema sejam comunicadas ao pessoal pertinente e às partes interessadas de forma pertinente, acessível e compreensível ao leitor pretendido. Convém que os destinatários das políticas sejam requeridos a reconhecer que entendem e concordam em cumprir as políticas quando aplicável. A organização pode determinar os formatos e nomes desses documentos de políticas que atendam às necessidades da organização. Em algumas organizações, a política de segurança da informação e políticas específicas por tema podem estar em um único documento. A organização pode nomear essas políticas específicas por tema para tópicos como normas, diretivas, políticas ou outras.

Se a política de segurança da informação ou qualquer política específica por tema for distribuída fora da organização, convém que os cuidados sejam tomados para não divulgar informações confidenciais.

A Tabela 1 ilustra as diferenças entre a política de segurança da informação e a política específica por tema.

Tabela 1 – Diferenças entre a política de segurança da informação e a política específica por tema

	Política de segurança da informação	**Política específica por tema**
Nível de detalhamento	Geral ou de alto nível	Específico ou detalhado
Formalmente aprovado e documentado por	Alta Direção	Nível apropriado de direção

Outras informações

As políticas específicas por tema podem variar entre as organizações.

5.2 Papéis e responsabilidades pela segurança da informação

Tipo de controle	**Propriedades de segurança da informação**	**Conceitos de segurança cibernética**	**Capacidades operacionais**	**Domínios de segurança**
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Identificar	#Governança	#Governança_e_ ecossistema #Proteção #Resiliência

Controle

Convém que os papéis e responsabilidades pela segurança da informação sejam definidos e alocados de acordo com as necessidades da organização.

Propósito

Estabelecer uma estrutura definida, aprovada e compreendida para a implementação, operação e gestão da segurança da informação dentro da organização.

Orientação

Convém que a alocação de papéis e responsabilidades pela segurança da informação seja feita de acordo com a política de segurança da informação e as políticas específicas por tema (ver 5.1). Convém que a organização defina e gerencie as responsabilidades por:

a) proteção de informações e outros ativos associados;

b) realização de processos específicos de segurança da informação;

c) atividades de gestão de riscos de segurança da informação e, em especial, aceitação de riscos residuais (por exemplo, para os proprietários de risco);

d) todo o pessoal usando as informações de uma organização e outros ativos associados.

Convém que essas responsabilidades sejam suplementadas, quando necessário, com orientações mais detalhadas para locais específicos e instalações de tratamento de informações. Indivíduos com responsabilidades definidas de segurança da informação podem atribuir tarefas de segurança a outras pessoas. No entanto, eles permanecem responsabilizáveis e convém que determinem que quaisquer tarefas delegadas estão sendo executadas corretamente.

Convém que cada área de segurança para a qual os indivíduos são responsáveis seja definida, documentada e comunicada. Convém que os níveis de autorização sejam definidos e documentados. Convém que os indivíduos que assumem um papel específico de segurança da informação sejam competentes nos conhecimentos e habilidades requeridos pela função e sejam apoiados para se manterem atualizados com os desenvolvimentos relacionados ao papel e que sejam necessários para cumprir as responsabilidades do papel.

Outras informações

Muitas organizações nomeiam um gestor de segurança da informação para assumir a responsabilidade global pelo desenvolvimento e implementação da segurança da informação e apoiar a identificação de riscos e controles mitigadores.

No entanto, a responsabilidade por pesquisar e implementar os controles frequentemente permanece com os gestores individuais. Uma prática comum é a nomeação de um proprietário para cada ativo que, então, se torna responsável por sua proteção no dia a dia.

Dependendo do tamanho e recursos de uma organização, a segurança da informação pode ser coberta por papéis dedicados ou ter as responsabilidades realizadas de forma adicional por papéis existentes.

5.3 Segregação de funções

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Governança #Gestão_de_ identidade_e_acesso	#Governança_e_ ecossistema

Controle

Convém que funções conflitantes e áreas de responsabilidade sejam segregados.

Propósito

Reduzir o risco de fraude, erro e desvio de controles de segurança da informação.

Orientação

A segregação de funções e áreas de responsabilidade visa separar as funções conflitantes entre diferentes indivíduos, a fim de evitar que um indivíduo execute potenciais funções conflitantes por conta própria.

Convém que a organização determine quais funções e áreas de responsabilidade precisam ser segregadas. Os seguintes são exemplos de atividades que podem exigir segregação:

a) iniciar, aprovar e executar uma mudança;

b) solicitar, aprovar e implementar os direitos de acesso;

c) projetar, implementar e revisar códigos;

d) desenvolver *software* e administrar os sistemas de produção;

e) utilizar e administrar as aplicações;

f) utilizar aplicações e administrar os bancos de dados;

g) projetar, auditar e garantir os controles de segurança da informação.

Convém que a possibilidade de conluio seja considerada na concepção dos controles de segregação. Pequenas organizações podem achar difícil alcançar a segregação de funções, mas convém que o princípio seja aplicado na medida do possível e praticável. Sempre que for difícil segregar, convém considerar outros controles, como monitoramento de atividades, trilhas de auditoria e supervisão da direção.

Convém que seja tomado cuidado ao usar sistemas de controle de acesso baseados em papéis para assegurar que não sejam concedidos papéis conflitantes para o pessoal. Quando há um grande número de funções, convém que as organizações considerem o uso de ferramentas automatizadas para identificar conflitos e facilitar sua remoção. Convém que os papéis sejam cuidadosamente definidos e provisionados para minimizar os problemas de acesso se um papel for removido ou redesignado.

Outras informações

Não há outra informação.

5.4 Responsabilidades da direção

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Identificar	#Governança	#Governança_e_ecossistema

Controle

Convém que a direção requeira que todo o pessoal aplique a segurança da informação de acordo com a política de segurança da informação estabelecida, com as políticas específicas por tema e com os procedimentos da organização.

Propósito

Assegurar que a direção entenda seu papel na segurança da informação e realize ações com o objetivo de assegurar que todo o pessoal esteja ciente e cumpra suas responsabilidades pela segurança da informação.

Orientação

Convém que a direção demonstre apoio à política de segurança da informação, políticas específicas por tema, procedimentos e controles de segurança da informação.

Convém que as responsabilidades da direção incluam a garantia de que o pessoal:

a) seja devidamente informado sobre seus papéis e responsabilidades de segurança da informação antes de ser concedido acesso às informações da organização e outros ativos associados;

b) tenha recebido as diretrizes que afirmam as expectativas de segurança da informação em seu papel dentro da organização;

c) seja obrigado a cumprir a política de segurança da informação e políticas específicas por tema da organização;

d) alcance um nível de consciência da segurança da informação relevante para seus papéis e responsabilidades dentro da organização (ver 6.3);

e) esteja de acordo com os termos e condições de trabalho, contrato ou acordo, incluindo a política de segurança da informação da organização e os métodos apropriados de trabalho;

f) continue a ter as habilidades e qualificações de segurança da informação adequadas através de educação profissional contínua;

g) sempre que possível, seja fornecido com um canal confidencial para relatar violações da política de segurança da informação, políticas específicas por temas ou procedimentos para segurança

da informação (“denúncia”). Isso pode permitir denúncias anônimas ou ter disposições para assegurar que o conhecimento da identidade do denunciante seja conhecido apenas por aqueles que precisam lidar com estes relatórios;

h) seja fornecido com recursos adequados e tempo de planejamento de projetos para a implementação dos processos e controles relacionados à segurança da organização.

Outras informações

Não há outra informação.

5.5 Contato com autoridades

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo #Corretivo	#Confidencialidade #Integridade #Disponibilidade	#Identificar #Proteger #Responder #Recuperar	#Governança	#Defesa #Resiliência

Controle

Convém que a organização estabeleça e mantenha contato com as autoridades relevantes.

Propósito

Assegurar o fluxo adequado de informações referentes à segurança da informação entre a organização e as autoridades legais, regulatórias e fiscalizadoras relevantes.

Orientação

Convém que a organização especifique quando e por quem é recomendado que as autoridades (por exemplo, os representantes da lei, os órgãos reguladores, as autoridades de supervisão) sejam contatadas e como é recomendado que os incidentes identificados de segurança da informação sejam relatados em tempo hábil.

Convém que os contatos com autoridades também sejam usados para facilitar o entendimento sobre as expectativas atuais e futuras dessas autoridades (por exemplo, regulamentações de segurança da informação aplicáveis).

Outras informações

As organizações sob ataque podem solicitar que as autoridades tomem medidas contra a fonte de ataque.

Manter esses contatos pode ser um requisito para apoiar a gestão de incidentes de segurança da informação (ver 5.24 a 5.28) ou o processo de planejamento de contingência e continuidade de negócios (ver 5.29 e 5.30). Os contatos com órgãos reguladores também são úteis para antecipar e se preparar para as próximas mudanças nas leis ou regulamentos relevantes que afetam a organização. Os contatos com outras autoridades incluem serviços públicos, serviços de emergência, fornecedores de energia elétrica e de saúde e segurança [por exemplo, corpo de bombeiros (em conexão com

a continuidade de negócios), provedores de telecomunicações (em conexão com roteamento e disponibilidade de linhas) e fornecedores de água (em conexão com instalações de resfriamento para equipamentos)].

5.6 Contato com grupos de interesse especial

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo #Corretivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger #Responder #Recuperar	#Governança	#Defesa

Controle

Convém que a organização estabeleça e mantenha contato com grupos de interesse especial ou outros fóruns de especialistas em segurança e associações profissionais.

Propósito

Assegurar que ocorra o fluxo adequado de informações relacionadas à segurança da informação.

Orientação

Convém que a adesão a grupos ou fóruns de interesse especial seja considerada como um meio para:

a) melhorar o conhecimento sobre as melhores práticas e manter-se atualizado com as informações relevantes sobre segurança;

b) assegurar que a compreensão do ambiente de segurança da informação esteja atual;

c) receber avisos antecipados de alertas, aconselhamentos e correções relativos a ataques e vulnerabilidades;

d) obter acesso a consultoria especializada em segurança da informação;

e) compartilhar e trocar informações sobre novas tecnologias, produtos, serviços, ameaças ou vulnerabilidades;

f) fornecer contatos adequados quando lidar com incidentes de segurança da informação (ver 5.24 a 5.28).

Outras informações

Não há outra informação.

5.7 Inteligência de ameaças

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo #Detectivo #Corretivo	#Confidencialidade #Integridade #Disponibilidade	#Identificar #Detectar #Responder	#Gestão_de_ameaças_e_vulnerabilidades	#Defesa #Resiliência

Controle

Convém que as informações relacionadas a ameaças à segurança da informação sejam coletadas e analisadas para produzir inteligência de ameaças.

Propósito

Conscientizar sobre o ambiente de ameaças da organização para que as ações de mitigação adequadas possam ser tomadas.

Orientação

Informações sobre ameaças existentes ou emergentes são coletadas e analisadas com objetivo de:

a) facilitar ações informadas para evitar que as ameaças causem danos à organização;

b) reduzir o impacto dessas ameaças.

A inteligência de ameaças pode ser dividida em três camadas, e convém que todas sejam consideradas:

a) inteligência estratégica de ameaças: troca de informações de alto nível sobre o cenário de ameaças em mudança (por exemplo, tipos de atacantes ou tipos de ataques);

b) inteligência tática de ameaças: informações sobre as metodologias dos atacantes, ferramentas e tecnologias envolvidas;

c) inteligência operacional de ameaças: detalhes sobre ataques específicos, incluindo indicadores técnicos.

Convém que a inteligência de ameaças seja:

a) relevante (ou seja, relacionada à proteção da organização);

b) perspicaz (ou seja, fornecendo à organização uma compreensão precisa e detalhada do cenário de ameaças);

c) contextual, para proporcionar consciência situacional (ou seja, agregar contexto às informações com base na sequência dos eventos, onde eles ocorreram, experiências anteriores e prevalência em organizações semelhantes);

d) acionável (ou seja, a organização pode agir sobre as informações de forma rápida e eficazmente).

Convém que as atividades de inteligência de ameaças incluam:

a) estabelecer os objetivos para a produção de inteligência de ameaças;

b) identificar, vetar e selecionar fontes de informação internas e externas que sejam necessárias e adequadas para fornecer as informações necessárias para a produção de inteligência de ameaças;

c) coletar informações de fontes selecionadas, que podem ser internas e externas;

d) tratar informações coletadas para prepará-las para análise (por exemplo, traduzindo, formatando ou corroborando as informações);

e) analisar a informação para entender como ela se relaciona e é significativa para a organização;

f) comunicar e compartilhá-la para indivíduos relevantes em um formato que possa ser entendido.

Convém que a inteligência de ameaças seja analisada e posteriormente usada:

a) por meio da implementação de processos para incluir informações coletadas de fontes de inteligência de ameaças nos processos de gestão de riscos de segurança da informação da organização;

b) como entrada adicional para controles técnicos preventivos e de detectivos, como *firewalls*, sistema de detecção de intrusões ou soluções *anti-malware*;

c) como entrada nos processos e técnicas de teste de segurança da informação.

Convém que as organizações compartilhem informações sobre inteligência de ameaças com outras organizações em uma base mútua, a fim de melhorar a inteligência geral de ameaças.

Outras informações

As organizações podem usar a inteligência de ameaças para prevenir, detectar ou responder a ameaças. As organizações podem produzir inteligência de ameaças, mas normalmente recebem e fazem uso de inteligência de ameaças produzida por outras fontes.

A inteligência de ameaças é frequentemente fornecida por provedores ou consultores independentes, agências governamentais ou grupos colaborativos de inteligência de ameaças.

A eficácia de controles como 5.25, 8.7, 8.16 ou 8.23, depende da qualidade da informação disponível sobre as ameaças.

5.8 Segurança da informação no gerenciamento de projetos

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Identificar #Proteger	#Governança	#Governança_e_ecossistema #Proteção

Controle

Convém que a segurança da informação seja integrada ao gerenciamento de projetos.

Propósito

Assegurar que os riscos de segurança da informação relacionados a projetos e entregas sejam efetivamente abordados no gerenciamento de projetos durante todo o ciclo de vida do projeto.

Orientação

Convém que a segurança da informação seja integrada ao gerenciamento de projetos para assegurar que os riscos de segurança da informação sejam abordados como parte do gerenciamento do projeto. Isso pode ser aplicado a qualquer tipo de projeto, independentemente de sua complexidade, tamanho, duração, disciplina ou área de aplicação (por exemplo, um projeto para um processo de negócios principal, TIC, gerenciamento de instalações ou outros processos de apoio).

Convém que o gerenciamento de projeto em uso requeira que:

a) os riscos de segurança da informação sejam avaliados e tratados em estágio inicial e periodicamente como parte dos riscos do projeto ao longo do ciclo de vida do projeto;

b) os requisitos de segurança da informação [por exemplo, requisitos de segurança de aplicações (8.26) e os requisitos para o cumprimento dos direitos de propriedade intelectual (5.32) etc.] sejam abordados nas fases iniciais dos projetos;

c) os riscos de segurança da informação associado à execução de projetos, como a segurança de aspectos de comunicação interna e externa, sejam considerados e tratados ao longo do ciclo de vida do projeto;

d) o progresso no tratamento de risco de segurança da informação seja analisado criticamente e a eficácia do tratamento seja avaliada e testada.

Convém que a adequação das considerações e atividades de segurança da informação seja acompanhada por pessoas ou órgãos diretivos adequados, como o comitê gestor do projeto, em etapas predefinidas.

Convém que as responsabilidades e autoridades pela segurança da informação sejam definidas e alocadas para papéis especificados.

Convém que os requisitos de segurança da informação para produtos ou serviços sejam entregues pelo projeto e sejam determinados usando vários métodos, incluindo requisitos de conformidade derivados da política de segurança da informação, políticas específicas por tema e regulamentos específicos. Outros requisitos de segurança da informação podem ser derivados de atividades como modelagem de ameaças, análises criticas de incidentes, uso de limiares de vulnerabilidade ou planejamento de contingência, assegurando assim que a arquitetura e o projeto dos sistemas de informação sejam protegidos contra ameaças conhecidas com base no ambiente operacional.

Convém que os requisitos de segurança da informação sejam determinados para todos os tipos de projetos, não apenas para projetos de desenvolvimento de TIC. Convém que sejam considerados os seguintes requisitos:

a) quais informações estão envolvidas (determinação da informação), qual é o seu valor de segurança correspondente (classificação; ver 5.12) e o potencial impacto negativo nos negócios que podem resultar da falta de segurança adequada;

b) as necessidades de proteção necessárias de informações e outros ativos associados envolvidos, particularmente em termos de confidencialidade, integridade e disponibilidade;

c) o nível de confiança ou garantia necessário para a identidade reivindicada das entidades, a fim de derivar os requisitos de autenticação;

d) os processos de provisionamento e autorização de acesso, para clientes e outros potenciais usuários de negócios, bem como para usuários privilegiados ou técnicos, como membros relevantes do projeto, equipe de operação em potencial ou fornecedores externos;

e) informar os usuários de seus deveres e responsabilidades;

f) os requisitos derivados de processos de negócios, como registro e monitoramento de transações, requisitos de não repúdio;

g) os requisitos exigidos por outros controles de segurança da informação (por exemplo, interfaces para sistemas de registro e monitoramento ou sistemas de detecção de vazamento de dados);

h) o cumprimento do ambiente legal, estatutário, regulatório e contratual no qual a organização atua;

i) o nível de confiança ou garantia necessárias para que terceiros atendam à política de segurança da informação da organização e políticas de tópicos específicos, incluindo cláusulas de segurança relevantes em quaisquer acordos ou contratos.

Outras informações

Convém que a abordagem de desenvolvimento de projetos, como ciclo de vida em cascata ou ciclo de vida ágil, apoie a segurança da informação de forma estruturada que possa ser adaptada para se adequar à gravidade avaliada dos riscos de segurança da informação, com base no caráter do projeto. A consideração antecipada dos requisitos de segurança da informação para o produto ou serviço (por exemplo, nas etapas de planejamento e projeto), pode levar a soluções mais eficazes e econômicas para a qualidade e segurança da informação. A ISO 21500 e a ISO 21502 fornecem orientações sobre conceitos e processos de gerenciamento de projetos que são importantes para o desempenho de projetos.

A ABNT NBR ISO/IEC 27005 fornece orientações sobre o uso de processos de gestão de riscos para identificar controles para atender aos requisitos de segurança da informação.

5.9 Inventário de informações e outros ativos associados

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Identificar	#Gestão_de_ativos	#Governança_e_ecossistema #Proteção

Controle

Convém que um inventário de informações e outros ativos associados, incluindo proprietários, seja desenvolvido e mantido.

Propósito

Identificar as informações da organização e outros ativos associados, a fim de preservar a sua segurança da informação e atribuir a propriedade adequada.

Orientação

Inventário

Convém que a organização identifique suas informações e outros ativos associados e determine sua importância em termos de segurança da informação. Convém que a documentação seja mantida em inventários dedicados ou existentes, conforme apropriado.

Convém que o inventário de informações e outros ativos associados seja preciso, atualizado, consistente e alinhado com outros inventários. As opções para assegurar a exatidão de um inventário de informações e outros ativos associados incluem:

a) conduzir análises críticas regulares de informações identificadas e outros ativos associados contra o inventário de ativos;

b) impor automaticamente uma atualização de inventário no processo de instalação, alteração ou remoção de um ativo.

Convém que a localização de um ativo seja incluída no inventário conforme apropriado.

O inventário não precisa ser uma única lista de informações e outros ativos associados. Convém que o inventário seja mantido pelas funções relevantes, que pode ser visto como um conjunto de inventários dinâmicos, como inventários de ativos de informação, *hardware*, *software*, máquinas virtuais (VM), instalações, pessoal, competências, capacidades e registros.

Convém que cada ativo seja classificado de acordo com a classificação das informações (ver 5.12) associadas a esse ativo.

Convém que a granularidade do inventário de informações e outros ativos associados estejam em um nível adequado para as necessidades da organização. Às vezes, casos específicos de ativos no ciclo de vida da informação não são viáveis de serem documentados devido à natureza do ativo. Um exemplo de um ativo de curta duração é uma instância VM cujo ciclo de vida pode ser de curta duração.

Propriedade

Convém que para as informações identificadas e outros ativos associados, a propriedade do ativo seja atribuída a um indivíduo ou a um grupo e a classificação seja identificada (ver 5.12, 5.13). Convém que um processo para assegurar a cessão oportuna de propriedade de ativos seja implementada. Convém que a propriedade seja atribuída quando os ativos são criados ou quando os ativos são transferidos para a organização. Convém que a propriedade de ativos seja reatribuída conforme necessário quando os atuais proprietários de ativos deixarem ou mudarem de atribuições.

Deveres do proprietário

Convém que o proprietário do ativo seja responsável pela gestão adequada de um ativo ao longo de todo o ciclo de vida útil do ativo, assegurando que:

a) as informações e outros ativos associados sejam inventariados;

Documento impresso em 27/06/2023 22:08:50, de uso exclusivo de UNIVERSIDADE FEDERAL DO CEARÁ

b) as informações e outros ativos associados sejam devidamente classificados e protegidos;

c) a classificação seja analisada criticamente de forma periódica;

d) os componentes que apoiam os ativos tecnológicos estejam listados e vinculados, como banco de dados, armazenamento, componentes de *software* e subcomponentes;

e) os requisitos para o uso aceitável de informações e outros ativos associados (ver 5.10) estejam estabelecidos;

f) as restrições de acesso correspondam à classificação e que sejam eficazes e analisados criticamente de forma periódica;

g) as informações e outros ativos associados, quando excluídos ou descartados, sejam tratados de forma segura e removidos do inventário;

h) eles estejam envolvidos na identificação e gestão de riscos associados com o(s) seu(s) ativo(s);

i) eles apoiem o pessoal que tem os papéis e responsabilidades de gerenciar suas informações.

Outras informações

Inventários de informações e outros ativos associados são muitas vezes necessários para assegurar a proteção efetiva das informações e podem ser requeridos para outros fins, como saúde e segurança, seguros ou razões financeiras. Inventario de informações e outros ativos associados também apoiam a gestão de riscos, atividades de auditoria, gerenciamento de vulnerabilidades, resposta a incidentes e planejamento de recuperação.

Tarefas e responsabilidades podem ser delegadas (por exemplo, a um custodiante que cuida dos ativos diariamente), mas a pessoa ou grupo que os delegou permanece responsabilizada.

Pode ser útil designar grupos de informações e outros ativos associados que atuam em conjunto para fornecer um determinado serviço. Neste caso, o proprietário deste serviço é responsabilizado pela prestação do serviço, incluindo a operação de seus ativos.

Ver a ISO/IEC 19770-1, para obter informações adicionais sobre gestão de ativos de TI. Ver a ABNT NBR ISO 55001, para obter informações adicionais sobre gestão de ativos.

5.10 Uso aceitável de informações e outros ativos associados

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Gestão_de_ativos #Proteção_da_informação	#Governança_e_Ecossistema #Proteção

Controle

Convém que regras para o uso aceitável e procedimentos para o manuseio de informações e outros ativos associados sejam identificados, documentados e implementados.

Propósito

Assegurar que as informações e outros ativos associados sejam devidamente protegidos, usados e manuseados.

Orientação

Convém que pessoas e usuários externos que usem ou tenham acesso às informações da organização e outros ativos associados estejam conscientes dos requisitos de segurança da informação para proteger e lidar com as informações da organização e outros ativos associados. Convém que eles sejam responsáveis pelo uso de qualquer recurso de tratamento das informações.

Convém que a organização estabeleça uma política específica por tema sobre o uso aceitável de informações e outros ativos associados e comunique a qualquer pessoa que use ou manuseie informações e outros ativos associados. Convém que a política específica por tema sobre uso aceitável forneça uma direção clara sobre como espera-se que os indivíduos usem as informações e outros ativos associados. Convém que a política específica por tema declare:

a) comportamentos esperados e inaceitáveis dos indivíduos do ponto de vista de segurança da informação;

b) uso permitido e proibido de informações e outros ativos associados;

c) atividades de monitoramento que estão sendo realizadas pela organização.

Convém que os procedimentos de uso aceitáveis sejam elaborados para o ciclo de vida completo das informações de acordo com sua classificação (ver 5.12) e os riscos determinados. Convém que os seguintes itens sejam considerados:

a) restrições de acesso que apoiam os requisitos de proteção para cada nível de classificação;

b) manutenção de registro dos usuários autorizados de informações e outros ativos associados;

c) proteção de cópias temporárias ou permanentes de informações a um nível consistente com a proteção das informações originais;

d) armazenamento de ativos associados a informações de acordo com as especificações dos fabricantes (ver 7.8);

e) marcação clara de todas as cópias de mídia de armazenamento (eletrônico ou físico) para a atenção do destinatário autorizado (ver 7.10);

f) autorização de descarte de informações e outros ativos associados e métodos de descarte de apoio (ver 8.10).

Outras informações

Pode ser o caso de que os ativos em questão não pertençam diretamente à organização, como serviços públicos em nuvem. Convém que o uso desses ativos de terceiros e quaisquer ativos da organização associados a estes ativos externos (por exemplo, informações, *software*) sejam identificados como aplicáveis e controlados, por exemplo, por meio de acordos com provedores de serviços em nuvem. Convém que cuidados também sejam tomados quando um ambiente colaborativo de trabalho é usado.

5.11 Devolução de ativos

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Gestão_de_ativos	#Proteção

Controle

Convém que o pessoal e outras partes interessadas, conforme apropriado, devolvam todos os ativos da organização em sua posse após a mudança ou encerramento da contratação ou acordo.

Propósito

Proteger os ativos da organização como parte do processo de mudança ou encerramento da contratação ou acordo.

Orientação

Convém que o processo de alteração ou rescisão seja formalizado para incluir a devolução de todos os ativos físicos e eletrônicos previamente emitidos, de propriedade ou confiados à organização.

Nos casos em que o pessoal e outras partes interessadas comprem os equipamentos da organização ou utilizem seus próprios equipamentos pessoais, convém que sejam seguidos procedimentos para assegurar que todas as informações relevantes sejam rastreadas e transferidas para a organização e excluídas com segurança do equipamento (ver 7.14).

Nos casos em que o pessoal e outras partes interessadas tenham conhecimento importante das operações em andamento, convém que essas informações sejam documentadas e transferidas para a organização.

Durante o período de aviso prévio e posteriormente, convém que a organização impeça a cópia não autorizada de informações relevantes (por exemplo, propriedade intelectual) pelo pessoal que está sob aviso de rescisão.

Convém que a organização identifique e documente claramente todas as informações e outros ativos associados a serem devolvidos, que podem incluir:

a) dispositivos *endpoint* do usuário;

b) dispositivos de armazenamento portáteis;

c) equipamentos especializados;

d) *hardware* de autenticação (por exemplo, chaves mecânicas, *tokens* físicos e *smartcards*) para sistemas de informação, *sites* e arquivos físicos;

e) cópias físicas de informações.

Outras informações

Pode ser difícil devolver informações sobre ativos que não pertencem à organização. Nesses casos, é necessário restringir o uso de informações utilizando outros controles de segurança da informação, como gestão de direitos de acesso (5.18) ou uso de criptografia (8.24).

5.12 Classificação das informações

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Identificar	#Proteção_da_informação	#Proteção #Defesa

Controle

Convém que as informações sejam classificadas de acordo com as necessidades de segurança da informação da organização com base na confidencialidade, integridade, disponibilidade e requisitos relevantes das partes interessadas.

Propósito

Assegurar a identificação e o entendimento das necessidades de proteção das informações de acordo com a sua importância para a organização.

Orientação

Convém que organização estabeleça uma política específica por tema sobre classificação e comunicação de informações para todas as partes interessadas pertinentes.

Convém que a organização considere os requisitos de confidencialidade, integridade e disponibilidade no esquema de classificação.

Convém que as classificações e controles de proteção associados às informações considerem as necessidades dos negócios para compartilhar ou restringir informações, para proteger a integridade das informações e para assegurar a disponibilidade, bem como os requisitos legais relativos à confidencialidade, integridade ou disponibilidade das informações. Outros ativos que não sejam as informações também podem ser classificados em conformidade com a classificação das informações, que são armazenadas, processadas ou manuseadas ou protegidas pelo ativo.

Convém que os proprietários de informações sejam responsabilizados por sua classificação.

Convém que o regime de classificação inclua convenções para classificação e critérios para análise crítica da classificação ao longo do tempo. Convém que os resultados da classificação sejam atualizados de acordo com as alterações do valor, sensibilidade e criticidade das informações ao longo de seu ciclo de vida.

Convém que o esquema esteja alinhado à política específica por tema sobre controle de acesso (ver 5.1) e seja capaz de atender às necessidades específicas de negócios da organização.

A classificação pode ser determinada pelo nível de impacto que seu comprometimento teria para a organização. Convém que a cada nível definido no esquema seja dado um nome que faça sentido no contexto da aplicação do regime de classificação.

Convém que o esquema seja consistente em toda a organização e esteja incluído em seus procedimentos para que todos classifiquem as informações e apliquem outros ativos associados da mesma forma. Desta forma, todos têm uma compreensão comum dos requisitos de proteção e para que todos apliquem a proteção adequada.

O esquema de classificação utilizado dentro da organização pode ser diferente dos esquemas utilizados por outras organizações, mesmo que os nomes para níveis sejam semelhantes. Além disso, as informações que se movem entre as organizações podem variar de classificação dependendo de seu contexto em cada organização, mesmo que seus esquemas de classificação sejam idênticos. Portanto, os acordos com outras organizações que incluem o compartilhamento de informações podem incluir procedimentos para identificar a classificação dessas informações e interpretar os níveis de classificação de outras organizações. A correspondência entre diferentes esquemas pode ser determinada buscando equivalência nos métodos de manuseio e proteção associados.

Outras informações

A classificação fornece às pessoas que lidam com informações com uma indicação concisa de como manuseá-la e protegê-la. Criar grupos de informações com necessidades de proteção semelhantes e especificar procedimentos de segurança da informação que se aplicam a todas as informações em cada grupo facilita isso. Esta abordagem reduz as necessidades de avaliar riscos caso a caso e customizar o projeto de controles.

As informações podem deixar de ser sensíveis ou críticas após um determinado período de tempo. Por exemplo, quando as informações forem tornadas públicas, ela não tem mais requisitos de confidencialidade, mas ainda pode requerer proteção para suas propriedades de integridade e disponibilidade. Convém que esses aspectos sejam levados em conta, pois a superclassificação pode levar à implementação de controles desnecessários que resultem em despesas adicionais ou, pelo contrário, a subclassificação pode levar a controles insuficientes para proteger as informações de comprometimento.

Um exemplo de um esquema de classificação de confidencialidade de informações pode ser baseado em quatro níveis, conforme a seguir:

a) a divulgação não causa danos;

b) a divulgação causa pequenos danos à reputação ou pequenos impactos operacionais;

c) a divulgação tem um impacto significativo de curto prazo nas operações ou objetivos de negócios;

d) a divulgação tem um impacto sério em objetivos de negócios de longo prazo ou coloca a sobrevivência da organização em risco.

5.13 Rotulagem de informações

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Proteção_da_informação	#Defesa #Proteção

Controle

Convém que um conjunto adequado de procedimentos para rotulagem de informações seja desenvolvido e implementado de acordo com o esquema de classificação de informações adotado pela organização.

Propósito

Facilitar a comunicação da classificação das informações e apoio à automação da gestão e tratamento das informações.

Orientação

Convém que os procedimentos para rotulagem de informações abranjam informações e outros ativos associados em todos os formatos. Convém que a rotulagem reflita o regime de classificação estabelecido em 5.12. Convém que os rótulos sejam facilmente reconhecíveis. Convém que os procedimentos orientem onde e como as etiquetas são anexadas considerando como as informações são acessadas ou os ativos são tratados dependendo dos tipos de mídia de armazenamento. Os procedimentos podem definir:

a) casos em que a rotulagem é omitida (por exemplo, rotulagem de informações não confidenciais para reduzir cargas de trabalho);

b) como rotular informações enviadas ou armazenadas em meios eletrônicos ou físicos ou qualquer outro formato;

c) como lidar com casos em que a rotulagem não é possível (por exemplo, devido a restrições técnicas).

Exemplos de técnicas de rotulagem incluem:

a) rótulos físicos;

b) cabeçalhos e rodapés;

c) metadados;

d) marca d’água;

e) carimbos de borracha.

Convém que as informações digitais utilizem metadados para identificar, gerenciar e controlar as informações, especialmente no que diz respeito à confidencialidade. Convém que os metadados também permitam a busca eficiente e correta das informações. Convém que os metadados facilitem os sistemas para interagir e tomar decisões com base nos rótulos de classificação anexados.

Convém que os procedimentos descrevam como anexar metadados às informações, quais rótulos usar e como convém que os dados sejam tratados, de acordo com o modelo de informações da organização e a arquitetura de TIC.

Convém que os metadados adicionais relevantes sejam incorporados pelos sistemas quando eles tratam informações dependendo de suas propriedades de segurança da informação.

Convém que o pessoal e outras partes interessadas estejam cientes dos procedimentos de rotulagem.

Convém que todo o pessoal tenha treinamento necessário para assegurar que as informações sejam corretamente rotuladas e tratadas adequadamente.

Convém que a saída de sistemas que contenham informações classificadas como sensíveis ou críticas contenham um rótulo de classificação adequado.

Outras informações

A rotulagem de informações classificadas é um requisito fundamental para o compartilhamento de informações.

Outro metadado útil que pode ser anexado às informações é qual processo organizacional criou as informações e em que momento.

A rotulagem de informações e outros ativos associados às vezes pode ter efeitos negativos. Ativos classificados podem ser mais fáceis de identificar por pessoas mal intencionadas, para potencial uso indevido.

Alguns sistemas não rotulam arquivos individuais ou registros de banco de dados com sua classificação, mas protegem todas as informações no mais alto nível de classificação de qualquer uma das informações que contém ou são permitidas para conter. É comum nesses sistemas determinar e, em seguida, rotular informações quando são exportadas.

5.14 Transferência de informações

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Gestão_de_ativos #Proteção_da_informação	#Proteção

Controle

Convém que regras, procedimentos ou acordos de transferência de informações sejam implementados para todos os tipos de recursos de transferência dentro da organização e entre a organização e outras partes.

Propósito

Manter a segurança das informações transferidas dentro de uma organização e com qualquer parte interessada externa.

Orientação

Geral

Convém que a organização estabeleça e comunique uma política específica por tema sobre transferência de informações para todas as partes interessadas pertinentes. Convém que regras, procedimentos e acordos para proteger informações em trânsito reflitam a classificação das informações envolvidas. Convém que quando as informações forem transferidas entre a organização e terceiros, os acordos de transferência (incluindo a autenticação do destinatário) sejam estabelecidos e mantidos para proteger as informações em todas as formas em trânsito (ver 5.10).

A transferência de informações pode acontecer através de transferência eletrônica, transferência de mídia de armazenamento físico e transferência verbal.

Convém que para todos os tipos de transferência de informações, regras, procedimentos e acordos incluam:

a) controles projetados para proteger informações transferidas contra interceptação, acesso não autorizado, cópia, modificação, desvio, destruição e negação de serviço, incluindo níveis de controle de acesso proporcionais à classificação das informações envolvidas e quaisquer controles especiais necessários para proteger informações sensíveis, como o uso de técnicas criptográficas (ver 8.24);

b) controles para assegurar a rastreabilidade e não repúdio, incluindo a manutenção de uma cadeia de custódia de informações durante o trânsito;

c) identificação de contatos apropriados relacionados à transferência, incluindo proprietários de informações, proprietários de riscos, agentes de segurança e custodiantes de informações, conforme aplicável;

d) responsabilidades, incluindo responsabilidade cível em caso de incidentes de segurança da informação, como perda de mídia de armazenamento físico ou dados;

e) uso de um sistema de rotulagem acordado para informações sensíveis ou críticas, assegurando que o significado dos rótulos seja imediatamente compreendido e que as informações sejam adequadamente protegidas (ver 5.13);

f) confiabilidade e disponibilidade do serviço de transferência;

g) política específica por tema ou diretrizes sobre o uso aceitável de recursos de transferência de informações (ver 5.10);

h) diretrizes de retenção e descarte para todos os registros de negócios, incluindo mensagens;

NOTA A legislação e os regulamentos locais podem existir em relação à retenção e descarte de registros de negócios.

i) consideração de quaisquer outros requisitos legais, estatutários, regulamentares e contratuais relevantes (ver 5.31, 5.32, 5.33, 5.34) relacionados à transferência de informações (por exemplo, requisitos para assinaturas eletrônicas).

Transferência eletrônica

Convém que regras, procedimentos e acordos também considerem os seguintes itens ao usar instalações de comunicação eletrônica para transferência de informações:

a) detecção e proteção contra *malware* que pode ser transmitido através do uso de comunicações eletrônicas (ver 8.7);

b) proteção de informações eletrônicas sensíveis comunicadas que estão na forma de um anexo;

c) prevenção contra o envio de documentos e mensagens em comunicações para o endereço errado ou número;

d) obtenção de aprovação antes do uso de serviços públicos externos, como mensagens instantâneas, redes sociais, compartilhamento de arquivos ou armazenamento em nuvem;

e) níveis mais fortes de autenticação ao transferir informações através de redes de acesso público;

f) restrições associadas com os recursos de comunicação eletrônica (por exemplo, prevenindo encaminhamento automático de correio eletrônico para endereços de correio externos);

g) aconselhamento de pessoal e outras partes interessadas a não enviar SMS ou mensagens instantâneas com informações críticas, uma vez que elas podem ser lidas em locais públicos (e, portanto, por pessoas não autorizadas) ou armazenadas em dispositivos não adequadamente protegidos;

h) aconselhamento de pessoal e outras partes interessadas sobre os problemas de uso de máquinas de *fax* ou serviços, ou seja:

   1) acesso não autorizado a lojas de mensagens incorporadas para recuperar mensagens;

   2) programação deliberada ou acidental de máquinas para enviar mensagens para números específicos.

Transferência de mídia de armazenamento físico

Convém que ao transferir mídia de armazenamento físico (incluindo papel), regras, procedimentos e acordos também sejam incluídos:

a) responsabilidades para controlar e notificar transmissão, expedição e recebimento;

b) assegurar o endereçamento e o transporte corretos da mensagem;

c) embalagem protegendo o conteúdo de qualquer dano físico que possa surgir durante o trânsito e de acordo com as especificações de qualquer fabricante, por exemplo, protegendo contra quaisquer fatores ambientais que podem reduzir a eficácia da restauração de meios de armazenamento, como exposição ao calor, umidade ou campo eletromagnéticos; utilizando normas técnicas mínimas para embalagem e transmissão (por exemplo, o uso de envelopes opacos);

d) lista de serviços postais confiáveis autorizados, acordados pela direção;

e) normas de identificação de serviço postal;

f) dependendo do nível de classificação das informações nos meios de armazenamento a serem transportadas, utilização de controles evidentes ou resistentes a adulterações (por exemplo, sacos, recipientes);

g) procedimentos para verificar a identificação dos entregadores;

h) lista aprovada de terceiros que fornecem serviços de transporte ou postal, dependendo da classificação das informações;

i) manutenção de registros para identificação do conteúdo dos meios de armazenamento, a proteção aplicada, bem como o registro da lista de destinatários autorizados, os horários de transferência para os custodiantes de trânsito e o recebimento no destino.

Transferência verbal

Convém que para proteger a transferência verbal de informações, o pessoal e outras partes interessadas sejam lembrados de:

a) não ter conversas verbais confidenciais em locais públicos ou por canais de comunicação inseguros, uma vez que estes podem ser ouvidos por pessoas não autorizadas;

b) não deixar mensagens contendo informações confidenciais em secretárias eletrônicas ou mensagens de voz, uma vez que elas podem ser reproduzidas por pessoas não autorizadas, armazenadas em sistemas comunitários ou armazenadas incorretamente como resultado de discagem errada;

c) ser rastreado para o nível apropriado para ouvir a conversa;

d) assegurar que os controles apropriados de sala sejam implementados (por exemplo, à prova de som, porta fechada);

e) iniciar quaisquer conversas sensíveis com um aviso para que os presentes saibam o nível de classificação e quaisquer requisitos de tratamento do que estão prestes a ouvir.

Outras informações

Não há outra informação.

5.15 Controle de acesso

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Gestão_de_ identidade_e_acesso	#Proteção

Controle

Convém que as regras para controlar o acesso físico e lógico às informações e outros ativos associados sejam estabelecidas e implementadas com base nos requisitos de segurança da informação e de negócios.

Propósito

Assegurar o acesso autorizado e evitar o acesso não autorizado a informações e outros ativos associados.

Orientação

Convém que os proprietários de informações e outros ativos associados determinem os requisitos de segurança da informação e de negócios relacionados ao controle de acesso. Convém que uma política específica por tema sobre controle de acesso seja definida e considere esses requisitos e que seja comunicada a todas as partes interessadas pertinentes.

Convém que esses requisitos e a política específica por tema considerem o seguinte:

a) determinação de quais entidades requerem qual tipo de acesso às informações e outros ativos associados;

b) segurança de aplicações (ver 8.26);

c) acesso físico, que precisa ser apoiado por controles de entradas físicas adequados (ver 7.2, 7.3, 7.4);

d) disseminação e autorização de informações (por exemplo, o princípio da necessidade de conhecer) e classificação e níveis de segurança das informações (ver 5.10, 5.12, 5.13);

e) restrições ao acesso privilegiado (ver 8.2);

f) segregação de funções (ver 5.3);

g) legislação, regulamentos e quaisquer obrigações contratuais relativas à limitação de acesso a dados ou serviços (ver 5.31, 5.32, 5.33, 5.34, 8.3);

h) segregação das funções de controle de acesso (por exemplo, solicitação de acesso, autorização de acesso, administração de acesso);

i) autorização formal de solicitações de acesso (ver 5.16 e 5.18);

j) gestão dos direitos de acesso (ver 5.18);

k) registro (ver 8.15).

Convém que as regras de controle de acesso sejam implementadas definindo e mapeando os direitos e as restrições de acesso adequados às entidades pertinentes (ver 5.16). Uma entidade pode representar um usuário humano, bem como um item técnico ou lógico (por exemplo, uma máquina, dispositivo ou um serviço). Para simplificar o gerenciamento de controle de acesso, funções específicas podem ser atribuídas a grupos de entidades.

Convém que o seguinte seja considerado ao definir e implementar regras de controle de acesso:

a) consistência entre os direitos de acesso e a classificação das informações;

b) consistência entre os direitos de acesso e as necessidades e requisitos de segurança do perímetro físico;

c) considerar todos os tipos de conexões disponíveis em ambientes distribuídos para que as entidades só tenham acesso a informações e outros ativos associados, incluindo redes e serviços de rede, que estejam autorizados a usar;

d) considerar como os elementos ou fatores relevantes para o controle de acesso dinâmico podem ser refletidos.

Outras informações

Muitas vezes existem princípios abrangentes usados no contexto do controle de acesso. Dois dos princípios mais frequentemente usados são:

a) necessidade de conhecer: uma entidade só tem acesso às informações que essa entidade requer para executar suas tarefas (diferentes tarefas ou papéis significam diferentes informações de necessidade de conhecer e, portanto, diferentes perfis de acesso);

b) necessidade de uso: só é atribuído acesso a uma entidade à infraestrutura de tecnologia da informação onde uma necessidade clara está presente.

Convém que sejam tomados cuidado ao especificar as regras de controle de acesso a considerar:

a) estabelecimento de regras baseadas na premissa de menor privilégio, “Tudo é geralmente proibido a menos que expressamente permitido”, em vez da regra mais fraca, “Tudo é geralmente permitido a menos que expressamente proibido”;

b) alterações nos rótulos de informações (ver 5.13) que são iniciadas automaticamente pelos recursos de tratamento de informações e aquelas iniciadas a critério de um usuário;

c) alterações nas permissões do usuário que são iniciadas automaticamente pelo sistema de informações e aquelas iniciadas por um administrador;

d) quando definir e analisar criticamente de forma regular à aprovação.

Convém que as regras de controle de acesso sejam apoiadas por procedimentos documentados (ver 5.16, 5.17, 5.18, 8.2, 8.3, 8.4, 8.5, 8.18) e responsabilidades definidas (ver 5.2 e 5.17).

Existem várias maneiras de implementar o controle de acesso, como MAC (controle de acesso obrigatório), DAC (controle de acesso discricionário), RBAC (controle de acesso baseado em papel) e ABAC (controle de acesso baseado em atributos).

As regras de controle de acesso também podem conter elementos dinâmicos (por exemplo, uma função que avalia acessos passados ou valores específicos do ambiente). As regras de controle de acesso podem ser implementadas em diferentes granularidades, desde a cobertura de redes ou sistemas inteiros até campos de dados específicos e também podem considerar propriedades como a localização do usuário ou o tipo de conexão de rede que é usada para acesso. Esses princípios e a forma como o controle de acesso granular é definido podem ter um impacto significativo nos custos. Regras mais fortes e mais granularidade normalmente levam a um custo mais alto. Convém que os requisitos de negócios e considerações de risco sejam usados para definir quais regras de controle de acesso são aplicadas e qual granularidade é requerida.

5.16 Gestão de identidade

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Gestão_de_identidade_e_acesso	#Proteção

Controle

Convém que o ciclo de vida completo das identidades seja gerenciado.

Propósito

Permitir a identificação única de indivíduos e sistemas que acessam as informações da organização e outros ativos associados e para permitir a cessão adequada de direitos de acesso.

Orientação

Convém que os processos utilizados no contexto da gestão da identidade assegurem que:

a) para identidades atribuídas às pessoas, uma identidade específica está vinculada apenas a uma única pessoa para ser capaz de responsabilizar a pessoa por ações realizadas com essa identidade específica;

b) identidades atribuídas a várias pessoas (por exemplo, identidades compartilhadas) só são permitidas quando forem necessárias por razões de negócios ou operacionais e estão sujeitas à aprovação e documentação dedicadas;

c) identidades atribuídas a entidades não humanas estão sujeitas à aprovação adequadamente segregada e à supervisão independente em curso;

d) identidades são desativadas ou removidas em tempo hábil se não forem mais necessárias (por exemplo, se suas entidades associadas forem excluídas ou não mais utilizadas, ou se a pessoa ligada a uma identidade deixou a organização ou mudou o de papel);

e) em um domínio específico, uma única identidade é mapeada para uma única entidade [ou seja, o mapeamento de múltiplas identidades para a mesma entidade dentro do mesmo contexto (identidades duplicadas) é evitado];

f) registros de todos os eventos significativos sobre o uso e gestão de identidades de usuários e as informações de autenticação são mantidas.

Convém que as organizações tenham um processo de apoio para lidar com alterações nas informações relacionadas a identidades de usuário. Esses processos podem incluir a reverificação de documentos confiáveis relacionados à pessoa.

Ao usar identidades fornecidas ou emitidas por terceiros (por exemplo, credenciais de mídia social), convém que a organização assegure que as identidades de terceiros forneçam o nível de confiança necessário e quaisquer riscos associados sejam conhecidos e suficientemente tratados. Isso pode incluir controles relacionados a terceiros (ver 5.19) bem como controles relacionados às informações de autenticação associadas (ver 5.17).

Outras informações

Fornecer ou revogar o acesso a informações e outros ativos associados geralmente é um procedimento de várias etapas:

a) confirmar os requisitos de negócios para que uma identidade seja estabelecida;

b) verificar a identidade de uma entidade antes de alocá-las como uma identidade lógica;

c) estabelecer uma identidade;

d) configurar e ativar a identidade. Isso também inclui configuração e configuração inicial de serviços de autenticação relacionados;

e) fornecer ou revogar direitos de acesso específicos à identidade, com base na autorização apropriada ou decisões de direito (ver 5.18).

5.17 Informações de autenticação

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Gestão_de_ identidade_e_acesso	#Proteção

Controle

Convém que a alocação e a gestão de informações de autenticação sejam controladas por uma gestão de processo, incluindo aconselhar o pessoal sobre o manuseio adequado de informações de autenticação.

Propósito

Assegurar a autenticação adequada da entidade e evitar falhas nos processos de autenticação.

Orientação

Alocação de informações de autenticação

Convém que o processo de alocação e gestão assegure que:

a) senhas pessoais ou números de identificação pessoal (PIN) gerados automaticamente durante os processos de inscrição como informações temporárias de autenticação secreta não sejam fáceis de adivinhar e únicas para cada pessoa, e que os usuários sejam obrigados a alterá-las após o primeiro uso;

b) procedimentos sejam estabelecidos para verificar a identidade de um usuário antes de fornecer informações novas, de substituição ou de autenticação temporária;

c) informações de autenticação, incluindo informações de autenticação temporária, sejam transmitidas aos usuários de forma segura (por exemplo, em um canal autenticado e protegido) e que o uso de mensagens eletrônicas desprotegidas (texto claro) é evitado;

d) usuários reconhecem o recebimento de informações de autenticação;

e) informações de autenticação-padrão conforme predefinidas ou fornecidas pelos fornecedores são alteradas imediatamente após a instalação de sistemas ou *softwares*;

f) registros de eventos significativos relativos à alocação e gestão de informações de autenticação sejam mantidos e sua confidencialidade assegurada, e que o método de registro seja aprovado (por exemplo, usando uma ferramenta de cofre de senha aprovada).

Responsabilidades do usuário

Convém que qualquer pessoa com acesso ou usando informações de autenticação seja avisada para assegurar que:

a) informações de autenticação secreta, como senhas, são mantidas em sigilo. Informações de autenticação secreta pessoal não são compartilhadas com ninguém. As informações de autenticação

secreta utilizadas no contexto de identidades vinculadas a múltiplos usuários ou vinculadas a entidades não pessoais são compartilhadas exclusivamente com pessoas autorizadas;

b) informações de autenticação afetadas ou comprometidas são alteradas imediatamente após a notificação ou qualquer outra indicação de um comprometimento;

c) quando senhas são usadas como informações de autenticação, senhas fortes de acordo com as melhores práticas recomendadas são selecionadas, por exemplo:

   1) as senhas não se baseiam em qualquer coisa que outra pessoa possa facilmente adivinhar ou obter usando informações relacionadas à pessoa (por exemplo, nomes, números de telefone e datas de nascimento);

   2) as senhas não são baseadas em palavras de dicionário ou combinações dela;

   3) usar frases de senha fáceis de lembrar e tentar incluir caracteres alfanuméricos e especiais;

   4) as senhas têm um comprimento mínimo;

d) as mesmas senhas não são usadas em serviços e sistemas distintos;

e) a obrigação de seguir essas regras também são incluídas em termos e condições de emprego (ver 6.2).

Sistema de gerenciamento de senhas

Convém que quando as senhas forem usadas como informações de autenticação, o sistema de gerenciamento de senhas considere:

a) permitir que os usuários selecionem e alterem suas próprias senhas e incluam um procedimento de confirmação para resolver erros de entrada;

b) impor senhas fortes de acordo com as recomendações de boas práticas [ver c) de “Responsabilidades do Usuário];

c) forçar os usuários a alterarem suas senhas no primeiro *login*;

d) impor alterações de senha conforme necessário, por exemplo, após um incidente de segurança, ou após a rescisão ou mudança de emprego quando um usuário tiver senhas conhecidas para identidades que permanecem ativas (por exemplo, identidades compartilhadas);

e) impedir o reuso de senhas anteriores;

f) impedir o uso de senhas comumente usadas e nomes de usuário comprometidos, combinações de senhas de sistemas *hackeados*;

g) não exibir senhas na tela ao ser inserido;

h) armazenar e transmitir senhas de forma protegida.

Convém que a criptografia de senha e o *hashing* sejam realizados de acordo com técnicas criptográficas aprovadas para senhas (ver 8.24).

Outras informações

Senhas ou frases são um tipo de informação de autenticação comumente usada e são um meio comum de verificar a identidade de um usuário. Outros tipos de informações de autenticação são chaves criptográficas, dados armazenados em *tokens* de *hardware* (por exemplo, cartões inteligentes) que produzem códigos de autenticação e dados biométricos, como varreduras de íris ou impressões digitais. Informações adicionais podem ser encontradas na série ISO/IEC 24760.

Requerer mudança frequente de senhas pode ser problemático porque os usuários podem ficar irritados com as mudanças frequentes, esquecer novas senhas, anotar em locais inseguros ou escolher senhas inseguras. A provisão de sinal único (SSO) ou outras ferramentas de gestão de autenticação (por exemplo, cofres de senha) reduz a quantidade de informações de autenticação que os usuários são requeridos a proteger e, assim, pode aumentar a eficácia deste controle. No entanto, essas ferramentas também podem aumentar o impacto da divulgação de informações de autenticação.

Algumas aplicações exigem que senhas de usuário sejam atribuídas por uma autoridade independente. Nesses casos, a), c) e d) de “Sistema de gerenciamento de senhas” não se aplicam.

5.18 Direitos de acesso

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Gestão_de_ identidade_e_acesso	#Proteção

Controle

Convém que os direitos de acesso às informações e outros ativos associados sejam provisionados, analisados criticamente, modificados e removidos de acordo com a política de tema específico e regras da organização para o controle de acesso.

Propósito

Assegurar que o acesso às informações e outros ativos associados esteja definido e autorizado de acordo com os requisitos do negócio.

Orientação

Provisão e revogação dos direitos de acesso

Convém que o processo de provisionamento para atribuição ou revogação de direitos de acesso físico e lógico concedidos à identidade autenticada de uma entidade inclua:

a) obtenção de autorização do proprietário das informações e de outros ativos associados para o uso das informações e outros ativos associados (ver 5.9). A aprovação separada dos direitos de acesso pela direção também pode ser apropriada;

b) consideração dos requisitos do negócio e as regras e política específica por tema da organização sobre controle de acesso;

c) consideração da segregação de funções, incluindo a segregação dos papéis de aprovação e implementação dos direitos de acesso e separação de papéis conflitantes;

d) garantia de que os direitos de acesso sejam removidos quando alguém não precisar acessar as informações e outros ativos associados, em particular assegurando que os direitos de acesso dos usuários que deixaram a organização sejam removidos em tempo hábil;

e) consideração da ação de direitos temporários de acesso por um período limitado e revogação deles na data de validade, em especial para pessoal temporário ou acesso temporário exigido pelo pessoal;

f) verificação de se o nível de acesso concedido está de acordo com as políticas específicas por tema sobre controle de acesso (ver 5.15) e é consistente com outros requisitos de segurança da informação, como a segregação de funções (ver 5.3);

g) garantia de que os direitos de acesso sejam ativados (por exemplo, por prestadores de serviços) somente após a conclusão dos procedimentos de autorização bem sucedido;

h) manutenção de um registro central dos direitos de acesso concedidos a um ID do usuário (lógico ou físico) para acessar informações e outros ativos associados;

i) modificação dos direitos de acesso dos usuários que mudaram de função ou emprego;

j) remoção ou ajuste dos direitos de acesso físico e lógico, que podem ser feitos por remoção, revogação ou substituição de chaves, informações de autenticação, cartões de identificação ou assinaturas;

k) manutenção de um registro de alterações nos direitos lógicos e físicos de acesso dos usuários.

Análise crítica dos direitos de acesso

Convém que as análises críticas regulares dos direitos de acesso físico e lógico considerem o seguinte:

a) direitos de acesso dos usuários após qualquer alteração dentro da mesma organização (por exemplo, mudança de emprego, promoção, rebaixamento) ou rescisão do emprego (ver 6.1 a 6.5);

b) autorizações para direitos de acesso privilegiados.

Consideração antes de alteração ou rescisão do emprego

Convém que os direitos de acesso de um usuário às informações e outros ativos associados sejam analisados criticamente e ajustados ou removidos antes de qualquer alteração ou rescisão de emprego com base na avaliação de fatores de risco como:

a) se a rescisão ou alteração é iniciada pelo usuário ou pela direção e o motivo da rescisão;

b) as responsabilidades atuais do usuário;

c) o valor dos ativos atualmente acessíveis.

Outras informações

Convém que seja considerado o estabelecimento de funções de acesso ao usuário com base nos requisitos de negócios que resumem uma série de direitos de acesso em perfis típicos de acesso ao usuário. Solicitações de acesso e análise critica dos direitos de acesso são mais fáceis de gerenciar ao nível de tais funções do que no nível de direitos particulares.

Convém que seja dada consideração à inclusão de cláusulas em contratos de pessoal e contratos de serviços que especifique sanções se o acesso não autorizado for tentado por pessoal (ver 5.20, 6.2, 6.4, 6.6).

Em casos de rescisão iniciada pela direção, pessoas descontentes ou usuários de partes externas podem deliberadamente corromper informações ou sabotar os recursos de tratamento de informações. Em casos de pessoas que se demitem ou são demitidas, elas podem ser tentadas a coletar informações para uso futuro.

A clonagem é uma maneira eficiente de as organizações atribuirem acesso aos usuários. No entanto, convém que seja feito com cuidado com base em funções distintas identificadas pela organização, em vez de apenas clonar uma identidade com todos os direitos de acesso associados. A clonagem tem um risco inerente de resultar em direitos excessivos de acesso à informação e outros ativos associados.

5.19 Segurança da informação nas relações com fornecedores

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Identificar	#Segurança_nas_relações_com_fornecedores	#Governança_e_ecossistema #Proteção

Controle

Convém que processos e procedimentos sejam definidos e implementados para gerenciar a segurança da informação e os riscos associados com o uso dos produtos ou serviços dos fornecedores.

Propósito

Manter um nível acordado de segurança da informação nas relações com fornecedores.

Orientação

Convém que a organização estabeleça e comunique uma política específica por tema sobre relacionamentos com fornecedores a todas as partes interessadas pertinentes.

Convém que a organização identifique e implemente processos e procedimentos para enfrentar riscos de segurança associados ao uso de produtos e serviços prestados pelos fornecedores. Convém que isso também se aplique ao uso da organização de recursos de provedores de serviços em nuvem. Convém que esses processos e procedimentos incluam aqueles a serem implementados pela organização, bem como aqueles que a organização requer que o fornecedor implemente para o início do uso de produtos ou serviços de um fornecedor ou para o término do uso de produtos e serviços de um fornecedor, como:

a) identificar e documentar os tipos de fornecedores (por exemplo, serviços de TIC, logística, utilidades, serviços financeiros, componentes de infraestrutura de TIC) que podem afetar a confidencialidade, integridade e disponibilidade das informações da organização;

b) estabelecer como avaliar e selecionar fornecedores de acordo com a sensibilidade de informações, produtos e serviços (por exemplo, com análise de mercado, referências ao cliente, análise crítica de documentos, avaliações no local, certificações);

c) avaliar e selecionar produtos ou serviços do fornecedor que tenham controles adequados de segurança da informação e analisá-los criticamente; em particular, a precisão e a completeza dos controles implementados pelo fornecedor que assegure a integridade do tratamento de informações e informações do fornecedor e, consequentemente, a segurança da informação da organização;

d) definir as informações da organização, os serviços de TIC e a infraestrutura física que os fornecedores podem acessar, monitorar, controlar ou usar;

e) definir os tipos de componentes e serviços de infraestrutura de TIC fornecidos pelos fornecedores que podem afetar a confidencialidade, integridade e disponibilidade das informações da organização;

f) avaliar e gerenciar os riscos de segurança da informação associados a:

   1) o uso das informações da organização pelos fornecedores e outros ativos associados, incluindo riscos originário de potenciais fornecedores maliciosos;

   2) mau funcionamento ou vulnerabilidades dos produtos (incluindo componentes de *software* e subcomponentes utilizados nesses produtos) ou serviços prestados pelos fornecedores;

g) monitorar o *compliance* com os requisitos estabelecidos de segurança da informação para cada tipo de fornecedor e tipo de acesso, incluindo análise crítica de terceiros e validação do produto;

h) mitigar a não conformidade de um fornecedor, seja ela detectada por meio de monitoramento ou por outros meios;

i) tratar de incidentes e contingências associados a produtos e serviços de fornecedores, incluindo responsabilidades tanto da organização quanto dos fornecedores;

j) aplicar resiliência e, se necessário, medidas de recuperação e contingência para assegurar a disponibilidade do tratamento de informações e informações do fornecedor e, consequentemente, a disponibilidade das informações da organização;

k) conscientizar e treinar o pessoal da organização interagindo com o pessoal do fornecedor sobre regras adequadas de engajamento, políticas específicas por tema para processos e procedimentos e comportamentos baseados no tipo de fornecedor e no nível de acesso do fornecedor aos sistemas de informações da organização;

l) gerenciar a transferência necessária de informações, outros ativos associados e qualquer outra coisa que precise ser alterada e assegurar que a segurança da informação seja mantida durante todo o período de transferência;

m) requisitos para assegurar um término seguro do relacionamento com o fornecedor, incluindo:

   1) desprovisionamento dos direitos de acesso;

   2) tratamento de informações;

   3) determinação da propriedade intelectual desenvolvida durante o engajamento;

   4) portabilidade de informações em caso de alteração de fornecedor ou internalização;

   5) gerenciamento de registros;

6) devolução de ativos;

7) eliminação segura de informações e outros ativos associados;

8) requisitos de confidencialidade em andamento;

n) nível de segurança pessoal e segurança física esperado do pessoal e instalações do fornecedor.

Convém que sejam considerados os procedimentos para o tratamento contínuo de informações, caso o fornecedor não consiga fornecer seus produtos ou serviços (por exemplo, por causa de um incidente, pois o fornecedor não está mais no negócio, ou não fornece mais alguns componentes devido aos avanços tecnológicos), para evitar qualquer atraso na organização de produtos ou serviços de substituição (por exemplo, identificando um fornecedor alternativo com antecedência ou sempre usando fornecedores alternativos).

Outras informações

Nos casos em que não seja possível para uma organização colocar requisitos em um fornecedor, convém que a organização:

a) considere a orientação dada neste controle na tomada de decisões sobre a escolha de um fornecedor e seu produto ou serviço;

b) implemente controles compensatórios conforme necessário com base em um processo de avaliação de riscos.

As informações podem ser colocadas em risco por fornecedores com uma gestão inadequada de segurança da informação. Convém que os controles sejam determinados e aplicados para gerenciar o acesso do fornecedor às informações e outros ativos associados. Por exemplo, se houver uma necessidade especial de confidencialidade das informações, acordos de não divulgação ou técnicas criptográficas podem ser usados. Outros exemplos são os riscos de proteção de dados pessoais quando o contrato de fornecedor envolve transferência ou acesso a informações além das fronteiras. A organização precisa estar ciente de que a responsabilidade legal ou contratual pela proteção das informações permanece com a organização.

Os riscos também podem ser causados por controles inadequados de componentes de infraestrutura de TIC ou serviços prestados pelos fornecedores. Componentes ou serviços defeituosos ou vulneráveis podem causar violações de segurança da informação na organização ou em outra entidade (por exemplo, eles podem causar infecção por *malware*, ataques ou outros danos a entidades que não a organização).

Ver a ISO/IEC 27036-2 para obter mais detalhes.

5.20 Abordagem da segurança da informação nos contratos de fornecedores

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Identificar	#Segurança_nas_relações_com_fornecedores	#Governança_e_ecossistema #Proteção

Controle

Convém que requisitos relevantes de segurança da informação sejam estabelecidos e acordados com cada fornecedor com base no tipo de relacionamento com o fornecedor.

Propósito

Manter um nível acordado de segurança da informação nas relações com fornecedores.

Orientação

Convém que os acordos com fornecedores sejam estabelecidos e documentados para assegurar que haja um entendimento claro entre a organização e o fornecedor sobre as obrigações de ambas as partes de cumprir com os requisitos relevantes de segurança da informação.

Os seguintes termos podem ser considerados para inclusão nos acordos, a fim de atender aos requisitos identificados de segurança da informação:

a) descrição das informações a serem fornecidas ou acessadas e métodos de fornecimento ou acesso às informações;

b) classificação das informações de acordo com o esquema de classificação da organização (ver 5.10, 5.12, 5.13);

c) mapeamento entre o próprio esquema de classificação da organização e o esquema de classificação do fornecedor;

d) requisitos legais, estatutários, regulamentares e contratuais, incluindo proteção de dados, manuseio de dados pessoais (DP), direitos de propriedade intelectual e direitos autorais e uma descrição de como será assegurado que eles são atendidos;

e) obrigação de cada parte contratual de implementar um conjunto de controles acordados, incluindo controle de acesso, análise crítica de desempenho, monitoramento, relatos e auditorias, e as obrigações do fornecedor de estar em conformidade com os requisitos de segurança da informação da organização;

f) regras de uso aceitável de informações e outros ativos associados, incluindo uso inaceitável, se necessário;

g) procedimentos ou condições para autorização e remoção da autorização para uso das informações da organização e outros ativos associados por pessoal fornecedor (por exemplo, por meio de uma lista explícita de fornecedores autorizados a usar as informações da organização e outros ativos associados);

h) requisitos de segurança da informação em relação à infraestrutura de TIC do fornecedor; em particular, requisitos mínimos de segurança da informação para cada tipo de informação e tipo de acesso para servir de base para acordos individuais de fornecedores com base nas necessidades de negócio e critérios de risco da organização;

i) indenizações e correções por falha do contratante em atender aos requisitos;

j) requisitos e procedimentos de gestão de incidentes (especialmente notificação e colaboração durante a remediação de incidentes);

k) requisitos de treinamento e conscientização para procedimentos específicos e requisitos de segurança da informação (por exemplo, para resposta a incidentes, procedimentos de autorização);

l) disposições relevantes para a subcontratação, incluindo os controles que precisam ser implementados, como acordo sobre o uso de subfornecedores (por exemplo, exigindo tê-los sob as mesmas obrigações do fornecedor, exigindo ter uma lista de subfornecedores e notificação antes de qualquer alteração);

m) contatos relevantes, incluindo uma pessoa de contato para problemas de segurança da informação;

n) quaisquer requisitos de triagem, quando legalmente permitidos, para o pessoal do fornecedor, incluindo responsabilidades pela realização dos procedimentos de triagem e notificação se a triagem não tiver sido concluída ou se os resultados derem motivo para dúvida ou preocupação;

o) mecanismos de evidência e garantia de atestados de terceiros para requisitos relevantes de segurança da informação relacionados aos processos de fornecedores e um relatório independente sobre a eficácia dos controles;

p) direito de auditar os processos e controles do fornecedor relacionados ao acordo;

q) obrigação do fornecedor de entregar periodicamente um relatório sobre a eficácia dos controles e concordância sobre a correção oportuna das questões relevantes levantadas no relatório;

r) processos de resolução de defeitos e resolução de conflitos;

s) fornecimento de cópias de segurança alinhada com às necessidades da organização (em termos de frequência e tipo e localização de armazenamento);

t) garantia da disponibilidade de uma instalação alternativa (por exemplo, local de recuperação de desastres) não sujeita às mesmas ameaças que a instalação primária e considerações de controles de retorno (controles alternativos), caso os controles primários falhem;

u) processo de gestão de mudanças que assegure a notificação prévia à organização e a possibilidade de organização de não aceitar alterações;

v) controles de segurança física proporcionais à classificação das informações;

w) controles de transferência de informações para proteger as informações durante a transferência física ou transmissão lógica;

x) cláusulas de rescisão após a celebração do contrato, incluindo gerenciamento de registros, devolução de ativos, descarte seguro de informações e outros ativos associados e quaisquer obrigações de confidencialidade em curso;

y) provisão de um método de destruição segura das informações da organização armazenadas pelo fornecedor assim que não for mais necessária;

z) garantia, ao final do contrato, do apoio a outro fornecedor ou à própria organização.

Convém que as organizações estabeleçam e mantenham um registro de acordos com partes externas (por exemplo, contratos, memorando de entendimento, acordos de compartilhamento de informações) para acompanhar para onde suas informações estão indo. Convém que as organizações também analisem criticamente, validem e atualizem regularmente seus acordos com partes externas para assegurar que ainda sejam necessárias e adequadas para o propósito com cláusulas relevantes de segurança da informação.

Outras informações

Os acordos podem variar consideravelmente para diferentes organizações e entre os diferentes tipos de fornecedores. Portanto, convém que seja tomado cuidado para incluir todos os requisitos relevantes para lidar com os riscos de segurança da informação.

Para obter detalhes sobre os contratos de fornecedores, ver a série ISO/IEC 27036. Para contratos de serviços em nuvem, ver a série ISO/IEC 19086.

5.21 Gestão da segurança da informação na cadeia de fornecimento de TIC

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Identificar	#Segurança_nas_relações_com_fornecedores	#Governança_e_ecossistema #Proteção

Controle

Convém que processos e procedimentos sejam definidos e implementados para gerenciar riscos de segurança da informação associados à cadeia de fornecimento de produtos e serviços de TIC.

Propósito

Manter um nível acordado de segurança da informação nas relações com fornecedores.

Orientação

Convém que os seguintes tópicos sejam considerados para abordar a segurança da informação dentro da segurança da cadeia de fornecimento de TIC, além dos requisitos gerais de segurança da informação para as relações com fornecedores:

a) definir requisitos de segurança da informação para aplicar a aquisição de produtos ou serviços de TIC;

b) exigir que os fornecedores de serviços de TIC propaguem os requisitos de segurança da organização por toda a cadeia de fornecimento, se subcontratarem partes do serviço de TIC prestados à organização;

c) exigir que os fornecedores de produtos de TIC propaguem práticas de segurança adequadas por toda a cadeia de fornecimento, se esses produtos incluírem componentes comprados ou adquiridos de outros fornecedores ou outras entidades (por exemplo, desenvolvedores de *software* subcontratados e provedores de componentes de *hardware*);

d) solicitar que os fornecedores de produtos de TIC forneçam informações descrevendo os componentes de *software* utilizados nos produtos;

e) solicitar que os fornecedores de produtos de TIC forneçam informações descrevendo as funções de segurança implementadas em seus produtos e as configurações necessárias para a sua operação segura;

f) implementar um processo de monitoramento e métodos aceitáveis para validação de produtos e serviços de TIC em conformidade com os requisitos de segurança declarados, exemplos destes métodos de revisão de fornecedores podem incluir testes de penetração e prova ou validação de atestados de terceiros para as operações de segurança da informação do fornecedor;

g) implementar um processo de identificação e documentação de componentes de produtos ou serviços que sejam fundamentais para a manutenção da funcionalidade e, portanto, requerem maior atenção, escrutínio e acompanhamento necessários quando construídos fora da organização, especialmente se o fornecedor terceirizar partes de componentes de produtos ou serviços para outros fornecedores;

h) obter garantia de que componentes críticos e sua origem podem ser rastreados em toda a cadeia de fornecimento;

i) obter garantia de que os produtos de TIC entregues estão funcionando como esperado sem quaisquer características inesperadas ou indesejadas;

j) implementando processos para garantir que os componentes dos fornecedores sejam genuínos e sem alteração de sua especificação. As medidas de exemplo incluem rótulos antiadulteração, verificações de *hash*, criptográficos ou assinaturas digitais. O monitoramento para o desempenho fora da especificação pode ser um indicador de adulteração ou falsificações. Convém que a prevenção e detecção de adulteração seja implementada durante múltiplas etapas do ciclo de vida do desenvolvimento do sistema, incluindo projeto, desenvolvimento, integração, operações e manutenção;

k) obter garantia de que os produtos de TIC atingem níveis de segurança necessários, por exemplo, através de certificação formal ou um esquema de avaliação, como o Acordo de Reconhecimento de Critérios Comuns;

l) definir regras para o compartilhamento de informações sobre a cadeia de fornecimento e eventuais problemas e compromissos entre a organização e fornecedores;

m) implementar processos específicos para a gestão do ciclo de vida dos componentes de TIC e disponibilidade e riscos de segurança associados. Isso inclui gerenciar os riscos de os componentes não estarem mais disponíveis devido aos fornecedores não estarem mais no negócio ou fornecedores não mais fornecerem esses componentes devido aos avanços tecnológicos. Convém que seja considerada a identificação de um fornecedor alternativo e o processo de transferência de *software* e competência para o fornecedor alternativo.

Outras informações

As práticas específicas de gestão de riscos da cadeia de fornecimento de TIC são construídas em cima das práticas gerais de segurança da informação, qualidade, gerenciamento de projetos e engenharia de sistemas, mas não as substituem.

As organizações são aconselhadas a trabalhar com fornecedores para entender a cadeia de fornecimento de TIC e quaisquer assuntos que tenham um efeito importante sobre os produtos e serviços que estão sendo prestados. A organização pode influenciar as práticas de segurança da informação da cadeia de fornecimento de TIC, deixando claro em acordos com seus fornecedores os assuntos que convém que sejam abordados por outros fornecedores da cadeia de fornecimento de TIC.

Convém que as TIC sejam adquiridas a partir de fontes confiáveis. A confiabilidade do *software* e do *hardware* é uma questão de controle de qualidade. Embora geralmente não seja possível para uma

organização inspecionar os sistemas de controle de qualidade de seus fornecedores, ela pode fazer julgamentos confiáveis com base na reputação do fornecedor.

As cadeias de fornecimento de TIC, conforme abordado neste controle, incluem serviços em nuvem. Exemplos de cadeias de fornecimento de TIC são:

a) provisão de serviços em nuvem, onde o provedor de serviços em nuvem confia nos desenvolvedores de *software*, provedores de serviços de telecomunicações, provedores de *hardware*;

b) IoT, onde o serviço envolve os fabricantes de dispositivos, os provedores de serviços em nuvem (por exemplo, os operadores de plataforma de IoT), os desenvolvedores de aplicações móveis e *web*, o fornecedor de bibliotecas de *software*;

c) serviços de hospedagem, onde o provedor conta com *service desks* externos, incluindo primeiro, segundo e terceiro níveis de apoio.

Ver a ISO/IEC 27036-3 para obter mais detalhes, incluindo orientação para o processo de avaliação de risco.

As *tags* de identificação de *software* (SWID) também podem ajudar a alcançar uma melhor segurança da informação na cadeia de fornecimento, fornecendo informações sobre procedência de *software*. Ver a ISO/IEC 19770-2 para obter mais detalhes.

5.22 Monitoramento, análise crítica e gestão de mudanças dos serviços de fornecedores

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Identificar	#Segurança_nas_ relações_com_ fornecedores	#Governança_e_ecossistema #Proteção #Defesa #Garantia_de_ segurança_ da_informaçã

Controle

Convém que a organização monitore, analise criticamente, avalie e gerencie regularmente a mudança nas práticas de segurança da informação dos fornecedores e na prestação de serviços.

Propósito

Manter um nível acordado de segurança da informação e prestação de serviços em linha com os acordos com os fornecedores.

Orientação

Convém que o monitoramento, a análise crítica e a gestão de mudanças dos serviços de fornecedores assegurem que os termos e condições de segurança da informação dos acordos estejam conformes, incidentes de segurança da informação e problemas sejam gerenciados adequadamente e mudanças nos serviços de fornecedores ou status de empresa não afetem a prestação de serviços.

Convém que isso envolva um processo para gerenciar a relação entre a organização e o fornecedor para:

a) monitorar os níveis de desempenho do serviço para verificar a conformidade com os acordos;

b) monitorar as alterações feitas pelos fornecedores, incluindo:

   1) melhorias nos serviços atuais oferecidos;

   2) desenvolvimento de quaisquer novas aplicações e sistemas;

   3) modificações ou atualizações das políticas e procedimentos do fornecedor;

   4) controles novos ou alterados para resolver incidentes de segurança da informação e melhorar a segurança da informação;

c) monitorar mudanças nos serviços de fornecedores, incluindo:

   1) mudanças e aprimoramento das redes;

   2) uso de novas tecnologias;

   3) adoção de novos produtos ou versões ou lançamentos mais recentes;

   4) novas ferramentas e ambientes de desenvolvimento;

   5) alterações na localização física das instalações de serviço;

   6) mudança de subfornecedores;

   7) subcontratação de outro fornecedor;

d) analisar criticamente os relatórios de serviços produzidos pelo fornecedor e organizar reuniões regulares de progresso conforme requerido pelos acordos;

e) realizar auditorias de fornecedores e subcontratados, em conjunto com análise crítica de relatórios de auditores independentes, se disponíveis, e acompanhamento das questões identificadas;

f) fornecer informações sobre incidentes de segurança a informação e analisar criticamente essas informações conforme requerido pelos acordos e quaisquer diretrizes e procedimentos de suporte;

g) analisar criticamente trilhas de auditoria de fornecedores e registros de eventos de segurança da informação, problemas operacionais, falhas, rastreamento de falhas e disrupções relacionadas ao serviço prestado;

h) responder e gerenciar quaisquer eventos ou incidentes identificados de segurança da informação;

i) identificar vulnerabilidades de segurança da informação e gerenciá-las;

j) analisar criticamente aspectos de segurança da informação das relações do fornecedor com seus próprios fornecedores;

k) assegurar que o fornecedor mantenha a capacidade de serviço suficiente, juntamente com planos viáveis projetados para assegurar que os níveis de continuidade de serviço acordados sejam mantidos após grandes falhas de serviço ou desastre (ver 5.29, 5.30, 5.35, 5.36 e 8.14) ;

l) assegurar que os fornecedores atribuam responsabilidades para analisar criticamente o *compliance* e aplicar os requisitos dos acordos;

m) avaliar regularmente se os fornecedores mantêm níveis adequados de segurança da informação.

Convém que a responsabilidade de gerenciar as relações com fornecedores seja atribuída a um indivíduo ou equipe designados. Convém que sejam disponibilizadas habilidades técnicas e recursos suficientes para monitorar se os requisitos do acordo, em particular os requisitos de segurança da informação, estão sendo atendidos. Convém que ações adequadas sejam tomadas quando forem observadas deficiências na prestação do serviço.

Outras informações

Ver a ISO/IEC 27036-3 para obter mais detalhes.

5.23 Segurança da informação para uso de serviços em nuvem

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Segurança_nas_relações_com_fornecedores	#Governança_e_ecossistema #Proteger

Controle

Convém que os processos de aquisição, uso, gestão e saída de serviços em nuvem sejam estabelecidos de acordo com os requisitos de segurança da informação da organização.

Propósito

Especificar e gerenciar a segurança da informação para o uso de serviços em nuvem.

Orientação

Convém que a organização estabeleceça e comunique políticas específicas por tema sobre o uso de serviços em nuvem para todas as partes interessadas relevantes.

Convém que a organização defina e comunique como pretende gerenciar riscos de segurança da informação associados ao uso de serviços em nuvem. Pode ser uma extensão ou parte da abordagem existente de como a organização gerencia os serviços prestados por partes externas (ver 5.21 e 5.22).

O uso de serviços em nuvem pode envolver responsabilidade compartilhada pela segurança da informação e esforço colaborativo entre o provedor de serviços em nuvem e a organização que atua como cliente de serviço em nuvem. É essencial que as responsabilidades tanto para o provedor de serviços em nuvem quanto para a organização, atuando como cliente de serviço em nuvem, sejam definidas e implementadas adequadamente.

Convém que a organização defina:

a) todos os requisitos relevantes de segurança da informação associados ao uso dos serviços em nuvem;

b) critérios de seleção de serviços em nuvem e escopo do uso de serviços em nuvem;

c) papéis e responsabilidades relacionadas ao uso e gestão de serviços em nuvem;

d) quais controles de segurança da informação são gerenciados pelo provedor de serviços em nuvem e quais são gerenciados pela organização como cliente de serviço em nuvem;

e) como obter e utilizar recursos de segurança da informação fornecidos pelo provedor de serviços em nuvem;

f) como obter garantia sobre controles de segurança da informação implementados por provedores de serviços em nuvem;

g) como gerenciar controles, interfaces e mudanças nos serviços quando uma organização usa vários serviços em nuvem, particularmente de diferentes provedores de serviços em nuvem;

h) procedimentos para o tratamento de incidentes de segurança da informação que ocorrem em relação ao uso de serviços em nuvem;

i) sua abordagem para monitorar, analisar criticamente e avaliar o uso contínuo de serviços em nuvem para gerenciar riscos de segurança da informação;

j) como alterar ou parar o uso de serviços em nuvem, incluindo estratégias de saída para serviços em nuvem.

Os contratos de serviços em nuvem são muitas vezes predefinidos e não estão abertos à negociação. Para todos os serviços em nuvem, convém que a organização analise criticamente os contratos de serviços em nuvem com o provedor de serviços em nuvem. Convém que um acordo de serviço em nuvem aborde os requisitos de confidencialidade, integridade, disponibilidade e manuseio de informações da organização, com objetivos apropriados de nível de serviço em nuvem e objetivos qualitativos de serviço em nuvem. Convém que a organização também realize processos de avaliação de risco pertinentes para identificar os riscos associados ao uso do serviço em nuvem. Convém que quaisquer riscos residuais ligados ao uso do serviço em nuvem sejam claramente identificados e aceitos pela gestão apropriada da organização.

Convém que um acordo entre o provedor de serviços em nuvem e a organização, atuando como cliente do serviço em nuvem, inclua as seguintes disposições para a proteção dos dados da organização e disponibilidade de serviços:

a) prover soluções baseadas em padrões aceitos de mercado para a arquitetura e a infraestrutura;

b) gerenciar controles de acesso dos serviços em nuvem que atendam aos requisitos da organização;

c) implementar soluções de monitoramento e proteção de *malware*;

d) tratar e armazenar as informações sensíveis da organização em locais aprovados (por exemplo, determinado país ou região), dentro ou sujeito a uma jurisdição específica;

e) prover suporte dedicado em caso de incidente de segurança da informação no ambiente do serviço em nuvem;

f) assegurar que os requisitos de segurança da informação da organização sejam atendidos no caso de os serviços de nuvem serem subcontratados de um fornecedor externo (ou proibir que os serviços em nuvem sejam subcontratados);

g) apoiar a organização na coleta de provas digitais, considerando as leis e regulamentos para evidências digitais em diferentes jurisdições;

h) prover suporte e disponibilidade adequados de serviços dentro de um prazo adequado, quando a organização quiser sair do serviço em nuvem;

i) prover o *backup* necessário de dados e informações de configuração, gerenciando os *backups* com segurança conforme aplicável, com base nos recursos do provedor de serviços em nuvem usado pela organização atuando como cliente de serviço em nuvem;

j) fornecer e retornar informações como arquivos de configuração, código-fonte e dados que pertencem à organização, atuando como cliente de serviço em nuvem, quando solicitado durante a prestação do serviço ou no término do serviço.

Convém que a organização, atuando como cliente do serviço em nuvem, considere se é recomendado que o acordo requeira que os provedores de serviços em nuvem forneçam notificação antecipada antes de quaisquer alterações de impacto substantivo para o cliente, na forma como o serviço é entregue à organização, incluindo:

a) alterações na infraestrutura técnica (por exemplo, realocação, reconfiguração ou alterações no *hardware* ou *software*) que afetam ou alteram a oferta do serviço em nuvem;

b) tratamento ou armazenamento de informações em uma nova jurisdição geográfica ou legal;

c) uso de provedores de serviços em nuvem por pares ou outros subcontratados (incluindo alterar partes existentes ou usar novas partes).

Convém que a organização que utiliza serviços em nuvem mantenha contato próximo com seus provedores de serviços em nuvem. Esses contatos permitem a troca mútua de informações sobre segurança da informação para o uso dos serviços em nuvem, incluindo um mecanismo tanto para o provedor de serviços em nuvem quanto para a organização, atuando como cliente do serviço em nuvem, para monitorar cada característica do serviço e relatar falhas nos compromissos contidos nos acordos.

Outras informações

Este controle considera a segurança na nuvem do ponto de vista do cliente do serviço em nuvem.

Podem ser encontradas informações adicionais relacionadas aos serviços de nuvem nas ABNT NBR ISO/IEC 17788, ISO/IEC 17789 e ISO/IEC 22123-1. As especificidades relacionadas à portabilidade no apoio no suporte às estratégias de saída podem ser encontradas na ISO/IEC 19941. As especificidades relacionadas à segurança da informação e serviços de nuvem pública estão descritas na ABNT NBR ISO/IEC 27017. As especificidades relacionadas à proteção de dados pessoais em nuvens públicas que atuam como operador de dados pessoais são descritas na ABNT NBR ISO/IEC 27018. As relações com fornecedores para serviços em nuvem são cobertas pela ISO/IEC 27036-4 e os contratos de serviços em nuvem e seus conteúdos são tratados na série ISO/IEC 19086, com segurança e privacidade especificamente cobertas pela ISO/IEC 19086-4.

5.24 Planejamento e preparação da gestão de incidentes de segurança da informação

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Corretivo	#Confidencialidade #Integridade #Disponibilidade	#Responder #Recuperar	#Governança #Gestão_de_eventos_de_ segurança_da_ informação	#Defesa

Controle

Convém que a organização planeje e se prepare para gerenciar incidentes de segurança da informação definindo, estabelecendo e comunicando processos, papéis e responsabilidades de gestão de incidentes de segurança da informação.

Propósito

Assegurar uma resposta rápida, eficaz, consistente e ordenada aos incidentes de segurança da informação, incluindo a comunicação sobre eventos de segurança da informação.

Orientação

Papéis e responsabilidades

Convém que a organização estabeleça processos adequados de gestão de incidentes de segurança da informação. Convém que os papéis e responsabilidades para a realização dos procedimentos de gestão de incidentes sejam determinadas e efetivamente comunicadas às partes interessadas internas e externas relevantes.

Convém que seja considerado o seguinte:

a) estabelecer um método comum para relatar eventos de segurança da informação, incluindo ponto de contato (ver 6.8);

b) estabelecer um processo de gestão de incidentes para fornecer à organização capacidade de gestão de incidentes de segurança da informação, incluindo administração, documentação, detecção, triagem, priorização, análise, comunicação e coordenação de partes interessadas;

c) estabelecer um processo de resposta a incidentes para fornecer à organização a capacidade de avaliar, responder e aprender com incidentes de segurança da informação;

d) permitir apenas que o pessoal competente lide com as questões relacionadas a incidentes de segurança da informação dentro da organização. Convém que este pessoal seja provido com documentação do procedimento e treinamento periódico;

e) estabelecer um processo para identificar o treinamento, a certificação e o desenvolvimento profissional continuado, requeridos para o pessoal de resposta a incidentes.

Procedimentos de gestão de incidentes

Convém que os objetivos para a gestão de incidentes de segurança da informação sejam acordados com a gestão da organização e que seja assegurado que os responsáveis pela gestão de incidentes

de segurança da informação entendam as prioridades da organização para lidar com os incidentes de segurança da informação, incluindo prazo de resolução baseado na severidade e consequências potenciais. Convém que os procedimentos de gestão de incidentes sejam implementados para atender a esses objetivos e prioridades.

Convém que a gestão da organização assegure que um plano de gestão de incidentes de segurança da informação seja criado, considerando diferentes cenários e que procedimentos sejam desenvolvidos e implementados para as seguintes atividades:

a) avaliação de eventos de segurança da informação de acordo com critérios para o que constitui um incidente de segurança da informação;

b) monitoramento (ver 8.15 e 8.16), detecção (ver 8.16), classificação (ver 5.25), análise e relatório (ver 6.8) de eventos e incidentes de segurança da informação (por meios humanos ou automáticos);

c) gestão de incidentes de segurança da informação até a conclusão, incluindo resposta e escalonamento (ver 5.26), de acordo com o tipo e a categoria do incidente, possível ativação da gestão de crises e ativação de planos de continuidade, recuperação controlada de incidentes e comunicação às partes interessadas internas e externas;

d) coordenação com partes interessadas internas e externas, como autoridades, interesse externo grupos e fóruns, fornecedores e clientes (ver 5.5 e 5.6);

e) atividades de gestão de incidentes de registro;

f) tratamento de evidências digitais (ver 5.28);

g) análise de causas-raiz ou procedimentos *post-mortem*;

h) identificação de lições aprendidas e quaisquer melhorias nos procedimentos de gestão de incidentes ou controles de segurança da informação em geral que são necessários.

Procedimentos de emissão de relatórios

Convém que os procedimentos de emissão de relatórios incluam:

a) ações a serem tomadas em caso de um evento de segurança da informação (por exemplo, anotando todos os detalhes pertinentes imediatamente, como ocorrência de mau funcionamento e mensagens na tela, reportando imediatamente ao ponto de contato e tomando apenas ações coordenadas);

b) uso de formulários de incidentes para apoiar o pessoal a realizar todas as ações necessárias ao relatar incidentes de segurança da informação;

c) processos de *feedback* adequados para assegurar que essas pessoas que relatam eventos de segurança da informação sejam notificadas, na medida do possível, dos resultados após o incidente ter sido tratado e encerrado;

d) criação de relatórios de incidentes.

Convém que quaisquer requisitos externos sobre relato de incidentes às partes interessadas pertinentes dentro do prazo definido (por exemplo, requisitos de notificação de violação aos reguladores) sejam considerados na implementação de procedimentos de gestão de incidentes.

Outras informações

Incidentes de segurança da informação podem transcender fronteiras organizacionais e nacionais. Para responder a estes incidentes, é benéfico coordenar a resposta e compartilhar informações sobre esses incidentes com organizações externas conforme apropriado.

Orientações detalhadas sobre a gestão de incidentes de segurança da informação são fornecidas na ISO/IEC 27035.

5.25 Avaliação e decisão sobre eventos de segurança da informação

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Detectivo	#Confidencialidade #Integridade #Disponibilidade	#Detectar #Responder	#Gestão_evento_de_segurança_da_informação	#Defesa

Controle

Convém que a organização avalie os eventos de segurança da informação e decida se categoriza como incidentes de segurança da informação.

Propósito

Assegurar a efetiva categorização e priorização de eventos de segurança da informação.

Orientação

Convém que um esquema de categorização e priorização de incidentes de segurança da informação seja acordado para a identificação das consequências e prioridade de um incidente. Convém que o esquema inclua os critérios para categorizar os eventos como incidentes de segurança da informação. Convém que o ponto de contato avalie cada evento de segurança da informação usando o esquema acordado.

Convém que o pessoal responsável pela coordenação e resposta a incidentes de segurança da informação realize a avaliação e tome uma decisão sobre eventos de segurança da informação.

Convém que os resultados da avaliação e da decisão sejam registrados em detalhes para fins de referência futura e verificação.

Outras informações

A série ISO/IEC 27035 fornece mais orientações sobre a gestão de incidentes.

5.26 Resposta a incidentes de segurança da informação

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Corretivo	#Confidencialidade #Integridade #Disponibilidade	#Responder #Recuperar	#Gestão_de_evento_de_ segurança_da_ informação	#Defesa

Controle

Convém que os incidentes de segurança da informação sejam respondidos de acordo com os procedimentos documentados.

Propósito

Assegurar uma resposta eficiente e eficaz aos incidentes de segurança da informação.

Orientação

Convém que a organização estabeleça e comunique os procedimentos de resposta aos incidentes de segurança da informação para todas as partes interessadas pertinentes.

Convém que os incidentes de segurança da informação sejam respondidos por uma equipe designada com a competência necessária (ver 5.24).

Convém que a resposta inclua o seguinte:

a) contenção, se as consequências do incidente podem se espalhar, dos sistemas afetados pelo incidente;

b) coleta de evidências (ver 5.28) o mais rápido possível após a ocorrência;

c) escalonamento, conforme necessário, incluindo atividades de gestão de crises e possivelmente invocação de planos de continuidade de negócios (ver 5.29 e 5.30);

d) garantia de que todas as atividades de resposta envolvidas sejam devidamente registradas para análise posterior;

e) comunicação da existência do incidente de segurança da informação ou quaisquer detalhes relevantes deles a todas as partes interessadas internas e externas relevantes seguindo o princípio da necessidade de conhecer;

f) coordenação com partes internas e externas, como autoridades, grupos de interesse externo e fóruns, fornecedores e clientes para melhorar a eficácia da resposta e ajudar a minimizar as consequências para outras organizações;

g) uma vez que o incidente foi tratado com sucesso, formalmente fechá-lo e registrá-lo;

h) análise forense de segurança da informação, conforme necessário (ver 5.28);

i) análise pós-incidente para identificar a causa-raiz. Assegurar que seja documentada e comunicada de acordo com os procedimentos definidos (ver 5.27);

j) identificação e gestão de vulnerabilidades e fragilidades de segurança da informação, incluindo aquelas relacionadas com os controles que causaram, contribuíram ou falharam em prevenir o incidente.

Outras informações

A série ISO/IEC 27035 fornece mais orientações sobre a gestão de incidentes.

5.27 Aprendizado com incidentes de segurança da informação

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Identificar #Proteger	#Gestão_de_evento_segurança_da_informação	#Defesa

Controle

Convém que o conhecimento adquirido com incidentes de segurança da informação seja usado para fortalecer e melhorar os controles de segurança da informação.

Propósito

Reduzir a probabilidade ou as consequências de futuros incidentes.

Orientação

Convém que a organização estabeleça procedimentos para quantificar e monitorar os tipos, volumes e custos dos incidentes de segurança da informação.

Convém que as informações obtidas com a avaliação dos incidentes de segurança da informação sejam utilizadas para:

a) melhorar o plano de gestão de incidentes, incluindo cenários e procedimentos de incidentes (ver 5.24);

b) identificar incidentes recorrentes ou graves e suas causas para atualizar o processo de avaliação de risco de segurança da informação da organização e determinar e implementar controles adicionais necessários para reduzir a probabilidade ou as consequências de futuros incidentes semelhantes. Mecanismos para permitir que incluam a coleta, a quantificação e o monitoramento de informações sobre custos, volumes e tipos de incidentes;

c) melhorar o treinamento e a conscientização do usuário (ver 6.3) fornecendo exemplos do que pode acontecer, como responder a estes incidentes e como evitá-los no futuro.

Outras informações

A série ISO/IEC 27035 fornece mais orientações.

5.28 Coleta de evidências

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Corretivo	#Confidencialidade #Integridade #Disponibilidade	#Detectar #Responder	#Gestão_de_evento_de_segurança_da_informação	#Defesa

Controle

Convém que a organização estabeleça e implemente procedimentos para identificação, coleta, aquisição e preservação de evidências relacionadas a eventos de segurança da informação.

Propósito

Assegurar uma gestão consistente e eficaz das evidências relacionadas a incidentes de segurança da informação para fins de ações disciplinares e legais.

Orientação

Convém que os procedimentos internos sejam desenvolvidos e seguidos ao tratar de evidências relacionadas a eventos de segurança da informação para fins de ações disciplinares e legais. Convém que os requisitos de diferentes jurisdições sejam considerados para maximizar as chances de admissão em todas as jurisdições relevantes.

Em geral, convém que esses procedimentos para o gerenciamento de evidências forneçam instruções para a identificação, coleta, aquisição e preservação de evidências de acordo com diferentes tipos de mídia de armazenamento, dispositivos e *status* dos dispositivos (ou seja, ligados ou desligados). As evidências normalmente precisam ser coletadas de forma admissível nos tribunais nacionais apropriados ou em outro fórum disciplinar. Convém que seja possível demonstrar que:

a) os registros estão completos e não foram adulterados de forma alguma;

b) as cópias de evidências eletrônicas são provavelmente idênticas aos originais;

c) qualquer sistema de informação a partir do qual as evidências foram coletadas estava operando corretamente no momento em que a evidência foi registrada.

Convém que, quando disponível, certificação ou outros meios relevantes de qualificação de pessoal e ferramentas sejam empregados, de modo a fortalecer o valor das evidências preservadas.

As evidências digitais podem transcender os limites organizacionais ou jurisdicionais. Nesses casos, convém assegurar que a organização tenha o direito de coletar as informações necessárias como evidência digital.

Outras informações

Quando um evento de segurança da informação é detectado pela primeira vez, nem sempre é óbvio se o evento resultará ou não em ação judicial. Portanto, existe o perigo de que as evidências necessárias sejam destruídas intencionalmente ou acidentalmente antes que a gravidade do incidente seja realizada. É aconselhável envolver assessoria jurídica ou aplicação da lei no início de qualquer ação legal contemplada e tomar conselhos sobre as provas necessárias.

A ISO/IEC 27037 fornece definições e diretrizes para identificação, coleta, aquisição e preservação de evidências digitais.

A série ISO/IEC 27050 trata da descoberta eletrônica, que envolve o tratamento de informações armazenadas eletronicamente como evidência.

5.29 Segurança da informação durante a disrupção

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo #Corretivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger #Responder	#Continuidade	#Proteção #Resiliência

Controle

Convém que a organização planeje como manter a segurança da informação em um nível apropriado durante a disrupção.

Propósito

Proteger as informações e outros ativos associados durante a disrupção.

Orientação

Convém que a organização determine seus requisitos para adaptar os controles de segurança da informação durante a disrupção. Convém que os requisitos de segurança da informação sejam incluídos nos processos de gestão de continuidade de negócios.

Convém que os planos sejam desenvolvidos, implementados, testados, analisados criticamente e avaliados para manter ou restaurar a segurança das informações de processos críticos de negócios após disrupção ou falha. Convém que a segurança da informação seja restaurada no nível e nos prazos requeridos.

Convém que a organização implemente e mantenha:

a) controles de segurança da informação, sistemas e ferramentas de suporte dentro dos planos de continuidade de negócios e TIC;

b) processos para manter os controles de segurança da informação existentes durante a disrupção;

c) controles de compensação para controles de segurança da informação que não podem ser mantidos durante a disrupção.

Outras informações

No contexto da continuidade do negócio e do planejamento da continuidade da TIC, pode ser necessário adaptar os requisitos de segurança da informação dependendo do tipo de disrupção, em comparação com as condições normais de operação. Como parte da análise de impacto nos negócios e processo de avaliação de riscos realizados na gestão de continuidade de negócios, convém que as consequências da perda de confidencialidade e integridade das informações sejam consideradas e priorizadas, além da necessidade de manter a disponibilidade.

Informações sobre gestão de continuidade de negócios podem ser encontradas na ABNT NBR ISO 22313 e na ABNT NBR ISO 22301 e informações sobre análise de impacto nos negócios (BIA) podem ser encontradas na ABNT ISO/TS 22317.

5.30 Prontidão de TIC para continuidade de negócios

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Corretivo	#Disponibilidade	#Responder	#Continuidade	#Resiliência

Controle

Convém que a prontidão da TIC seja planejada, implementada, mantida e testada com base nos objetivos de continuidade de negócios e nos requisitos de continuidade da TIC.

Propósito

Assegurar a disponibilidade das informações da organização e outros ativos associados durante a disrupção.

Orientação

A prontidão de TIC para a continuidade dos negócios é um componente importante na gestão da continuidade de negócios e na gestão da segurança da informação para assegurar que os objetivos da organização possam continuar a ser cumpridos durante a disrupção.

Os requisitos de continuidade das TIC são o resultado da análise de impacto nos negócios (BIA). Convém que o processo BIA utilize tipos e critérios de impacto para avaliar os impactos ao longo do tempo decorrentes da disrupção das atividades empresariais que fornecem produtos e serviços. Convém que a magnitude e duração do impacto resultante sejam utilizadas para identificar atividades priorizadas que convém que sejam atribuídas a um objetivo de tempo de recuperação (RTO). Convém que a BIA então determine quais recursos são necessários para apoiar as atividades priorizadas. Convém que um RTO também seja especificado para esses recursos. Convém que um subconjunto desses recursos inclua serviços de TIC.

A BIA envolvendo serviços de TIC pode ser expandida para definir os requisitos de desempenho e capacidade dos sistemas de TIC e dos objetivos de ponto de recuperação (RPO) das informações necessárias para apoiar as atividades durante a disrupção.

Com base nas saídas da BIA e no processo de avaliação de risco envolvendo serviços de TIC, convém que a organização identifique e selecione estratégias de continuidade de TIC que considerem opções para antes, durante e após a disrupção. As estratégias de continuidade de negócios podem incluir uma ou mais soluções. Convém que, com base nas estratégias, os planos sejam desenvolvidos, implementados e testados para atender ao nível de disponibilidade requerido dos serviços de TIC e nos prazos requeridos após disrupção ou falha de processos críticos.

Convém que a organização assegure que:

a) existe uma estrutura organizacional adequada para preparar, mitigar e responder a uma disrupção, suportada por pessoal com a necessária responsabilidade, autoridade e competência;

b) planos de continuidade de TIC, incluindo procedimentos de resposta e recuperação detalhando como a organização está planejando gerenciar uma disrupção do serviço de TIC, sejam:

   1) regularmente avaliados por meio de exercícios e testes;

   2) aprovados pela direção;

c) Os planos de continuidade de TIC incluem as seguintes informações de continuidade de TIC:

   1) especificações de desempenho e capacidade para atender aos requisitos e objetivos de continuidade de negócios especificados na BIA;

   2) RTO de cada serviço de TIC priorizado e os procedimentos para a restauração desses componentes;

   3) RPO dos recursos priorizados de TIC definidos como informações e procedimentos para restauração da informação.

Outras informações

Gerenciar a continuidade de TIC forma uma parte fundamental dos requisitos de continuidade de negócios em relação à disponibilidade para ser capaz de:

a) responder e recuperar de disrupção dos serviços de TIC independentemente da causa;

b) assegurar que a continuidade das atividades priorizadas são apoiadas pelos serviços de TIC necessários;

c) responder antes que ocorra uma disrupção nos serviços de TIC, e após a detecção de pelo menos um incidente que pode resultar em uma disrupção nos serviços de TIC.

Orientações adicionais podem ser encontradas sobre a prontidão de TIC para a continuidade dos negócios na ISO/IEC 27031.

Orientações adicionais podem ser encontradas sobre o sistema de gestão de continuidade de negócios na ABNT NBR ISO 22301 e na ABNT NBR ISO 22313.

Orientações adicionais podem ser encontradas sobre BIA na ABNT ISO/TS 22317.

5.31 Requisitos legais, estatutários, regulamentares e contratuais

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventiva	#Confidencialidade #Integridade #Disponibilidade	#Identificar	#Legal_e_ *compliance*	#Governança_e_ ecossistema #Proteção

Controle

Convém que os requisitos legais, estatutários, regulamentares e contratuais pertinentes à segurança da informação e à abordagem da organização para atender a esses requisitos sejam identificados, documentados e atualizados.

Propósito

Assegurar o *compliance* dos requisitos legais, estatutários, regulamentares e contratuais relacionados à segurança da informação.

Orientação

Geral

Convém que os requisitos externos, incluindo requisitos legais, estatutários, regulamentares ou contratuais sejam considerados quando ocorrer:

a) desenvolvimento de políticas e procedimentos de segurança da informação;

b) projeto, implementação ou alteração de controles de segurança da informação;

c) classificação de informações e outros ativos associados como parte do processo de definição de requisitos de segurança da informação para necessidades internas ou para acordos de fornecedores;

d) realização de processos de avaliações de risco de segurança da informação e determinação de atividades de tratamento de risco de segurança da informação;

e) determinação de processos, juntamente com papéis e responsabilidades relacionados à segurança da informação;

f) determinação dos requisitos contratuais dos fornecedores relevantes para a organização e o escopo de fornecimento de produtos e serviços.

Legislação e regulamentos

Convém que a organização:

a) identifique todas as legislações e regulamentos pertinentes à segurança da informação da organização, a fim de estar ciente dos requisitos para o seu tipo de negócio;

b) considere o *compliance* em todos os países pertinentes, se a organização:

   — realizar negócios em outros países;

   — usar produtos e serviços de outros países onde leis e regulamentos podem afetar a organização;

   — transferir informações através de fronteiras jurisdicionais onde leis e regulamentos podem afetar a organização;

c) analise criticamente a legislação e a regulamentação identificadas regularmente, a fim de manter-se atualizada com as mudanças e identifique novas legislações;

d) defina e documente os processos específicos e responsabilidades individuais para atender a esses requisitos.

Criptografia

Criptografia é uma área que muitas vezes tem requisitos legais específicos. Convém que o *compliance* com acordos, leis e regulamentos pertinentes relativos aos seguintes itens considere:

a) restrições à importação ou exportação de *hardware* e *software* de computador para a execução de funções criptográficas;

b) restrições à importação ou exportação de *hardware* e *software* de computador que foi projetado para ter funções criptográficas adicionadas a ele;

c) restrições ao uso de criptografia;

d) métodos obrigatórios ou discricionários de acesso pelas autoridades dos países às informações criptografadas;

e) validade de assinaturas digitais, selos e certificados.

Recomenda-se buscar aconselhamento jurídico ao assegurar *compliance* com a legislação e regulamentos pertinentes, especialmente quando informações criptografadas ou ferramentas de criptografia são movidas através das fronteiras jurisdicionais.

Contratos

Convém que os requisitos contratuais relacionados à segurança da informação incluam aqueles indicados em:

a) contratos com clientes;

b) contratos com fornecedores (ver 5.20);

c) contratos de seguro.

Outras informações

Não há outra informação.

5.32 Direitos de propriedade intelectual

Tipo de controle	Informação propriedades de segurança	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Identificar	#Legal_e_ *compliance*	#Governança_e_ ecossistema

Controle

Convém que a organização implemente procedimentos adequados para proteger os direitos de propriedade intelectual.

Propósito

Assegurar o *compliance* dos requisitos legais, estatutários, regulamentares e contratuais relacionados aos direitos de propriedade intelectual e ao uso de produtos proprietários.

Orientação

Convém que as seguintes diretrizes sejam consideradas para proteger qualquer material que possa ser considerado propriedade intelectual:

a) definir e comunicar uma política específica por tema sobre proteção dos direitos de propriedade intelectual;

b) publicar procedimentos para o *compliance* dos direitos de propriedade intelectual que definam o uso adequado de *software* e produtos de informação;

c) adquirir *software* somente por meio de fontes conhecidas e confiáveis, para assegurar que os direitos autorais não sejam violados;

d) manter registros apropriados de ativos e identificar todos os ativos com requisitos de proteção de direitos de propriedade intelectual;

e) manter provas e evidências de propriedade de licenças, manuais etc.;

f) assegurar que qualquer número máximo de usuários ou recursos (por exemplo, CPU) permitidos dentro da licença não seja excedido;

g) realizar análises críticas para assegurar que apenas *softwares* autorizados e produtos licenciados sejam instalados;

h) fornecer procedimentos para a manutenção das condições adequadas de licença;

i) fornecer procedimentos para descartar ou transferir *software* para terceiros;

j) manter o *compliance* dos termos e condições de *software* e informações obtidas de redes públicas e fontes externas;

k) não duplicar, converter para outro formato ou extrair de gravações comerciais (vídeo, áudio) outro além do permitido pela lei de direitos autorais e as licenças aplicáveis;

l) não copiar, total ou parcialmente, normas (por exemplo, normas internacionais ISO/IEC), livros, artigos, relatórios ou outros documentos, além do permitido pela lei de direitos autorais e as licenças aplicáveis.

Outras informações

Os direitos de propriedade intelectual incluem direitos autorais de *software* ou documentos, direitos de *design*, marcas comerciais, patentes e licenças de código fonte.

Os produtos de *software* proprietários geralmente são fornecidos sob um contrato de licença que especifica termos e condições de licença, por exemplo, limitando o uso dos produtos a máquinas especificadas ou limitando a cópia apenas à criação de cópias de *backup*. Ver a ISO/IEC 19770 para obter detalhes sobre a gestão de ativos de TI.

Os dados podem ser adquiridos de fontes externas. É geralmente o caso de que estes dados são obtidos nos termos de um acordo de compartilhamento de dados ou instrumento legal semelhante. Convém que esses acordos de compartilhamento de dados deixem claro qual o tratamento permitido para os dados adquiridos. Também é aconselhável que a procedência dos dados seja claramente declarada. Ver a ISO/IEC 23751 para obter detalhes sobre acordos de compartilhamento de dados.

Requisitos legais, estatutários, regulamentares e contratuais podem colocar restrições à cópia de material proprietário. Em particular, eles podem requerer que apenas material que é desenvolvido pela organização ou que seja licenciado ou fornecido pelo desenvolvedor para a organização, seja usado. A violação de direitos autorais pode levar a ações judiciais, que podem envolver multas e processos criminais.

Além da organização que precisa cumprir suas obrigações em relação aos direitos de propriedade intelectual de terceiros, convém que os riscos de pessoal e terceiros não cumprirem os direitos de propriedade intelectual da própria organização também sejam gerenciados.

5.33 Proteção de registros

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Identificar #Proteger	#Legal_e_ *compliance* #Gestão_de_ativos #Proteção_da_ informação	#Defesa

Controle

Convém que os registros sejam protegidos contra perdas, destruição, falsificação, acesso não autorizado e liberação não autorizada.

Propósito

Assegurar o *compliance* dos requisitos legais, estatutários, regulamentares e contratuais, bem como expectativas comunitárias ou sociais relacionadas à proteção e disponibilidade de registros.

Orientação

Convém que a organização tome as seguintes medidas para proteger a autenticidade, confiabilidade, integridade e usabilidade dos registros, enquanto seu contexto de negócios e os requisitos para a sua administração mudam ao longo do tempo:

a) emitir diretrizes sobre o armazenamento, manuseio da cadeia de custódia e descarte de registros, o que inclui a prevenção da manipulação de registros. Convém que essas diretrizes estejam alinhadas com a política específica por tema da organização sobre gerenciamento de registros e outros requisitos de registros;

b) elaborar um cronograma de retenção definindo registros e o período de tempo pelo qual convém que eles sejam retidos.

Convém que o sistema de armazenamento e manuseio assegure a identificação dos registros e do seu período de retenção levando em consideração a legislação ou regulamentos nacionais ou regionais, bem como as expectativas comunitárias ou sociais, se aplicável. Convém que este sistema permita a destruição adequada dos registros após esse período, se eles não forem necessários pela organização.

Ao decidir sobre a proteção de registros organizacionais específicos, convém considerar sua classificação correspondente de segurança da informação, com base no esquema de classificação da organização. Convém que os registros sejam categorizados em tipos de registros (por exemplo, registros contábeis, registros de transações comerciais, registros pessoais, registros legais), cada um com detalhes de períodos de retenção e tipo de mídia de armazenamento permitida, que pode ser física ou eletrônica.

Convém que os sistemas de armazenamento de dados sejam escolhidos de forma que os registros necessários possam ser recuperados em um período e formato aceitáveis, dependendo dos requisitos a serem cumpridos.

Convém que, quando as mídias de armazenamento eletrônico forem escolhidas, procedimentos para assegurar a capacidade de acessar registros (mídia de armazenamento e legibilidade de formato), durante todo o período de retenção, sejam estabelecidos, para proteger contra perdas devido à futura mudança de tecnologia. Convém que quaisquer chaves criptográficas e programas relacionados associados a arquivos criptografados ou assinaturas digitais também sejam retidos para permitir a descriptografia dos registros pelo tempo que os registros são retidos (ver 8.24).

Convém que os procedimentos de armazenamento e manuseio sejam implementados de acordo com as recomendações fornecidas pelos fabricantes de mídia de armazenamento. Convém considerar a possibilidade de deterioração dos meios utilizados para armazenamento de registros.

Outras informações

Os registros documentam eventos ou transações individuais ou podem formar agregações que foram projetadas para documentar processos de trabalho, atividades ou funções. Ambos são evidências de atividade empresarial e ativos de informação. Qualquer conjunto de informações, independentemente de sua estrutura ou forma, pode ser gerenciado como um registro. Isso inclui informações na forma de um documento, uma coleta de dados ou outros tipos de informações digitais ou analógicas que são criadas, capturadas e gerenciadas no decorrer dos negócios.

Na gestão dos registros, metadados são dados que descrevem o contexto, conteúdo e estrutura dos registros, bem como sua gestão ao longo do tempo. Metadados são componentes essenciais de qualquer registro.

Pode ser necessário reter alguns registros com segurança para atender aos requisitos legais, estatutários, regulamentares ou contratuais, bem como apoiar atividades comerciais essenciais. A lei ou regulamento nacional pode definir o período de tempo e o conteúdo dos dados para retenção de informações. Mais informações sobre o gerenciamento de registros podem ser encontradas na ISO 15489.

5.34 Privacidade e proteção de DP

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Identificar #Proteger	#Proteção_da_informação #Legal_e_ *compliance*	#Proteção

Controle

Convém que a organização identifique e atenda aos requisitos relativos à preservação da privacidade e proteção de DP de acordo com as leis e regulamentos aplicáveis e requisitos contratuais.

Propósito

Assegurar o *compliance* dos requisitos legais, estatutários, regulamentares e contratuais relacionados aos aspectos de segurança da informação da proteção de DP.

Orientação

Convém que a organização estabeleça e comunique uma política específica por tema sobre privacidade e proteção de DP para todas as partes interessadas relevantes.

Documento impresso em 27/06/2023 22:08:50, de uso exclusivo de UNIVERSIDADE FEDERAL DO CEARÁ

Convém que a organização desenvolva e implemente procedimentos para a preservação da privacidade e proteção de DP. Convém que esses procedimentos sejam comunicados a todas as partes interessadas relevantes envolvidas no tratamento de DP.

O *compliance* desses procedimentos e todas as legislações e regulamentos pertinentes relativos à preservação da privacidade e proteção de DP exige papéis, responsabilidades e controles adequados. Muitas vezes isso é melhor obtido com a nomeação de um responsável, como um Encarregado de Proteção de Dados. Convém que o Encarregado de Proteção de Dados forneça orientação ao pessoal, provedores de serviços e outras partes interessadas sobre suas responsabilidades individuais e os procedimentos específicos que convém que sejam seguidos.

Convém que a responsabilidade de lidar com os DP seja tratada de acordo com a legislação e os regulamentos pertinentes.

Convém que medidas técnicas e organizacionais adequadas para proteger DP sejam implementadas.

Outras informações

Vários países introduziram legislação que coloca controles sobre a coleta, tratamento, transmissão e exclusão de DP. Dependendo da respectiva legislação nacional, tais controles podem impor deveres àqueles que coletam, tratam e divulgam DP e também podem restringir a autoridade para transferir DP para outros países.

A ABNT NBR ISO/IEC 29100 fornece uma estrutura de alto nível para a proteção de DP dentro dos sistemas de TIC. Mais informações sobre sistemas de gestão da privacidade de informações podem ser encontradas na ABNT NBR ISO/IEC 27701. Informações específicas sobre a gestão de privacidade de informações para nuvens públicas que atuam como operadores de DP podem ser encontradas na ABNT NBR ISO/IEC 27018.

A ABNT NBR ISO/IEC 29134 fornece diretrizes para avaliação de impacto de privacidade (PIA) e um exemplo da estrutura e conteúdo de um relatório PIA. Em comparação com a ABNT NBR ISO/IEC 27005, ela é focada no tratamento de DP e pertinente para as organizações que tratam DP. Isso pode ajudar a identificar riscos de privacidade e possíveis mitigações para reduzir esses riscos a níveis aceitáveis.

5.35 Análise crítica independente da segurança da informação

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo #Corretivo	#Confidencialidade #Integridade #Disponibilidade	#Identificar #Proteger	#Garantia_de_ segurança_ da_ informação	#Governança_e_ ecossistema

Controle

Convém que a abordagem da organização para gerenciar a segurança da informação e sua implementação, incluindo pessoas, processos e tecnologias, seja analisada criticamente de forma independente a intervalos planejados ou quando ocorrem mudanças significativas.

Propósito

Assegurar a contínua adequação, suficiência e eficácia da abordagem da organização para a gestão da segurança da informação.

Orientação

Convém que a organização tenha processos para realizar análises críticas independentes.

Convém que a direção planeje e inicie análises críticas periódicas. Convém que as análises críticas incluam a avaliação de oportunidades de melhoria e a necessidade de mudanças na abordagem da segurança da informação, incluindo a política de segurança da informação, políticas de temas específicos e outros controles.

Convém que essas análises críticas sejam realizadas por indivíduos independentes da área em análise (por exemplo, a função de auditoria interna, um gestor independente ou uma organização externa especializada em tais análises críticas). Convém que os indivíduos que realizam essas análises críticas tenham a competência adequada. Convém que a pessoa que conduz as análises críticas não esteja na linha de autoridade para assegurar que ela tenha a independência para fazer uma avaliação.

Convém que os resultados das análises críticas independentes sejam informados ao gestor que iniciou as análises críticas e, se for o caso, à Alta Direção. Convém que esses registros sejam mantidos.

Convém que a gestão implemente as ações corretivas, se as análises críticas independentes identificarem que a abordagem e a implementação da organização para a gestão da segurança da informação são inadequadas [por exemplo, objetivos e requisitos documentados não são atendidos ou não estão de acordo com o direcionamento de segurança da informação indicado na política de segurança da informação e políticas de temas específicos (ver 5.1)],

Além das análises críticas independentes periódicas, convém que a organização considere a realização de análises críticas independentes quando:

a) leis e regulamentos que afetem a organização mudarem;

b) incidentes significativos ocorrerem;

c) a organização iniciar um novo negócio ou mudar um negócio atual;

d) a organização começar a usar um novo produto ou serviço, ou alterar o uso de um produto atual ou serviço;

e) a organização alterar significativamente os controles e procedimentos de segurança da informação.

Outras informações

A ABNT NBR ISO/IEC 27007 e a ISO/IEC TS 27008 fornecem orientações para a realização de análises críticas independentes.

5.36 Conformidade com políticas, regras e normas para segurança da informação

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Identificar #Proteger	#Legal_e_*compliance* #Garantia_de_segurança_da_informação	#Governança_e_ecossistema

Controle

Convém que o *compliance* da política de segurança da informação da organização, políticas, regras e normas de temas específicos seja analisado criticamente a intervalos regulares.

Propósito

Assegurar que a segurança da informação seja implementada e operada de acordo com a política de segurança da informação da organização, políticas, regras e normas específicas por tema.

Orientação

Convém que gestores, proprietários de serviços, produtos ou informações identifiquem como analisar criticamente os requisitos de segurança da informação definidos na política de segurança da informação, políticas específicas por tema, regras, normas e outras regulamentações aplicáveis. Convém que ferramentas automáticas de medição e emissão de relatórios sejam consideradas para uma análise crítica regular eficiente.

Se qualquer não *compliance* for encontrado como resultado da análise crítica, convém que os gestores:

a) identifiquem as causas do não *compliance*;

b) avaliem a necessidade de ações corretivas para alcançar o *compliance*;

c) implementem ações corretivas adequadas;

d) analisem criticamente as ações corretivas tomadas para verificar sua eficácia e identificar quaisquer deficiências ou fragilidades.

Convém que os resultados das análises críticas e ações corretivas realizadas pelos gestores, proprietários de serviços, produtos ou informações sejam registrados e que registros sejam mantidos. Convém que os gestores informem os resultados às pessoas que realizam análises críticas independentes (ver 5.35) quando uma análise crítica independente ocorre na área de sua responsabilidade.

Convém que as ações corretivas sejam concluídas em tempo hábil, conforme apropriado ao risco. Se não for concluída até a próxima análise crítica programada, convém que o progresso, pelo menos, seja abordado nessa análise crítica.

Outras informações

O monitoramento operacional do uso do sistema é coberto em 8.15, 8.16, 8.17.

5.37 Documentação dos procedimentos de operação

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo #Corretivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger #Recuperar	#Gestão_de_ativos #Segurança_fisica #Segurança_de_sistemas_e_ rede #Segurança_de_aplicações #Configuração_segura #Gestão_de_identidade_e_acesso #Gestão_de_ameaças_e_vulnerabilidades #Continuidade #Gestão_de_evento_de_segurança_da_informação	#Governança_e_ecossistema #Proteção #Defesa

Controle

Convém que os procedimentos de operação dos recursos de tratamento da informação sejam documentados e disponibilizados para o pessoal que necessite deles.

Propósito

Assegurar a operação correta e segura dos recursos de tratamento da informação.

Orientação

Convém que procedimentos documentados sejam preparados para as atividades operacionais da organização associadas com segurança da informação, por exemplo:

a) quando a atividade precisa ser realizada da mesma forma por muitas pessoas;

b) quando a atividade é realizada raramente e na próxima vez que tiver que ser realizada provavelmente foi esquecida;

c) quando a atividade é nova e apresenta um risco se não for realizada corretamente;

d) antes de entregar a atividade para pessoal novo.

Convém que os procedimentos operacionais especifiquem:

a) as responsabilidades individuais;

b) a instalação e configuração seguras dos sistemas;

c) o tratamento e manuseio de informações, tanto automatizados quanto manuais;

d) o *backup* (ver 8.13) e resiliência;

e) os requisitos de agendamento, incluindo interdependências com outros sistemas;

f) as instruções para o manuseio de erros ou outras condições excepcionais [por exemplo, restrições ao uso de programas utilitários (ver 8.18)], que podem surgir durante a execução do trabalho;

g) os contatos de suporte e escalonamento, incluindo contatos de suporte externo em caso de dificuldades operacionais ou técnicas inesperadas;

h) as instruções de manuseio de mídia de armazenamento (ver 7.10 e 7.14);

i) os procedimentos de reinicialização e recuperação do sistema para uso em caso de falha do sistema;

j) a gestão das informações de trilha de auditoria e *log* do sistema (ver 8.15 e 8.17) e monitoramento de sistemas de vídeo (ver 7.4);

k) os procedimentos de monitoramento como capacidade, desempenho e segurança (ver 8.6 e 8.16);

l) as instruções de manutenção.

Convém que os procedimentos operacionais documentados sejam analisados criticamente e atualizados quando necessário. Convém que alterações nos procedimentos operacionais documentados sejam autorizadas. Quando tecnicamente possível, convém que os sistemas de informação sejam gerenciados de forma consistente, utilizando os mesmos procedimentos, ferramentas e infraestrutura.

Outras informações

Não há outra informação.

6 Controles de pessoas

6.1 Seleção

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Segurança_em_ recursos_humanos	#Governança_e_ ecossistema

Controle

Convém que verificações de antecedentes de todos os candidatos a serem contratados sejam realizadas antes de ingressarem na organização e de modo contínuo, de acordo com as leis, regulamentos e ética aplicáveis e que sejam proporcionais aos requisitos do negócio, à classificação das informações a serem acessadas e aos riscos percebidos.

Propósito

Assegurar que todo o pessoal seja elegível e adequado para os papéis para os quais são considerados e permaneça elegível e adequado durante sua contratação.

Orientação

Convém que um processo de seleção seja realizado para todo o pessoal, incluindo pessoas em tempo integral, meio período e temporários. Convém que quando esses indivíduos forem contratados por meio de fornecedores de serviços, os requisitos de validação sejam incluídos nos acordos contratuais entre a organização e os fornecedores.

Convém que as informações sobre todos os candidatos que estão sendo considerados para cargos dentro da organização sejam coletadas e tratadas de acordo com qualquer legislação adequada existente na jurisdição competente. Em algumas jurisdições, a organização pode ser legalmente requerida a informar os candidatos antecipadamente sobre as atividades de seleção.

Convém que a verificação considere toda a legislação relevante de privacidade, proteção de DP e trabalhista e, quando permitido, inclua o seguinte:

a) disponibilidade de referências satisfatórias (por exemplo, referências empresariais e pessoais);

b) verificação (da completeza e exatidão) do *curriculum vitae* do candidato;

c) confirmação de qualificações acadêmicas e profissionais alegadas;

d) verificação independente de identidade (por exemplo, passaporte ou outro documento aceitável emitido pelas autoridades competentes);

e) verificação mais detalhada, como análise crítica de crédito ou análise crítica de registros criminais, se o candidato for admitido para uma função crítica.

Quando um indivíduo é contratado para um papel específico de segurança da informação, convém que as organizações assegurem que o candidato:

a) tenha a competência necessária para o papel de segurança;

b) possa ser confiável para assumir a função, especialmente se a função é fundamental para a organização.

Convém que a organização considere realizar verificações mais detalhadas onde um trabalho envolva pessoas, seja na contratação ou em promoção, que tenham acesso a recursos de tratamento de informações e, em particular, se isso envolve o manuseio de informações confidenciais (por exemplo, informações financeiras, informações pessoais ou informações de saúde).

Convém que os procedimentos definam critérios e limitações para análises críticas de verificação (por exemplo, quem é elegível para selecionar pessoas e como, quando e por que as análises críticas de verificação são realizadas).

Em situações em que não é possível concluir a verificação em tempo hábil, convém que os controles mitigadores sejam implementados até que a análise crítica seja concluída, por exemplo:

a) atraso na integração;

b) atraso na implantação de ativos corporativos;

c) integração com acesso reduzido;

d) rescisão de emprego.

Convém que as verificações sejam repetidas periodicamente para confirmar a adequação contínua do pessoal, dependendo da criticidade das funções de cada pessoa.

Outras informações

Não há outra informação.

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Segurança_em_ recursos_humanos	#Governança_e_ ecossistema

6.2 Termos e condições de contratação

Controle

Convém que os contratos trabalhistas declarem as responsabilidades do pessoal e da organização para a segurança da informação.

Propósito

Assegurar que o pessoal entenda suas responsabilidades de segurança da informação para os papéis para os quais eles são considerados.

Orientação

Convém que as cláusulas contratuais para o pessoal considerem a política de segurança da informação da organização e políticas de temas específicos relevantes. Além disso, os seguintes pontos podem ser esclarecidos e declarados:

a) convém que acordos de confidencialidade ou não divulgação sejam assinados antes de o pessoal que tem acesso a informações confidenciais ter acesso a informações e outros ativos associados (ver 6.6);

b) responsabilidades e direitos legais [por exemplo, sobre leis de direitos autorais ou legislação de proteção de dados (ver 5.32 e 5.34)];

c) responsabilidades para a classificação de informações e gestão de informações da organização e outros ativos associados, recursos de tratamento de informações e serviços de informação manuseados pelo pessoal (ver 5.9 a 5.13);

d) responsabilidades para o manuseio das informações recebidas das partes interessadas;

e) ações a serem tomadas se o pessoal não cumprir os requisitos de segurança da organização (ver 6.4).

Convém que os papéis e responsabilidades de segurança da informação sejam comunicados aos candidatos durante o processo de seleção.

Convém que a organização assegure que o pessoal concorde com os termos e condições relativos à segurança da informação. Convém que esses termos e condições sejam adequados à natureza e extensão do acesso que eles terão aos ativos da organização associados a sistemas e serviços de informação. Convém que os termos e condições relativos à segurança da informação sejam analisados criticamente quando leis, regulamentos, política de segurança da informação ou políticas específicas por tema mudarem.

Onde apropriado, convém que as responsabilidades contidas nos termos e condições da contratação continuem por um período definido após o término da contratação (ver 6.5).

Outras informações

Um código de conduta pode ser usado para declarar as responsabilidades de segurança da informação do pessoal em relação à confidencialidade, proteção de DP, ética, uso adequado das informações da organização e outros ativos associados, bem como práticas respeitáveis esperadas pela organização.

Uma entidade externa, com a qual o pessoal do fornecedor está associado, pode ser solicitada a celebrar acordos contratuais em nome do indivíduo contratado.

Se a organização não é uma pessoa jurídica e não tem empregados, o equivalente ao acordo contratual e aos termos e condições podem ser considerados em linha com a orientação deste controle.

6.3 Conscientização, educação e treinamento em segurança da informação

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Segurança_em_ recursos_humanos	#Governança_e_ ecossistema

Controle

Convém que o pessoal da organização e partes interessadas relevantes recebam treinamento, educação e conscientização em segurança da informação apropriados e atualizações regulares da política de segurança da informação da organização, políticas e procedimentos específicas por tema, pertinentes para as suas funções.

Propósito

Assegurar que o pessoal e as partes interessadas pertinentes estejam cientes e cumpram suas responsabilidades de segurança da informação.

Orientação

Geral

Convém que um programa de conscientização, educação e treinamento em segurança da informação seja estabelecido de acordo com a política de segurança da informação da organização, políticas de específicas por tema e procedimentos relevantes sobre segurança da informação, levando em consideração as informações da organização a serem protegidas e os controles de segurança da informação implementados para proteger as informações.

Convém que a conscientização, a educação e o treinamento em segurança da informação sejam realizados periodicamente. A conscientização, a educação e o treinamento iniciais podem se aplicar a pessoal novo e àqueles que se transferem para novos cargos ou funções com requisitos substancialmente diferentes de segurança da informação.

Convém que o entendimento do pessoal seja avaliado ao final de uma atividade de conscientização, educação ou treinamento para testar a transferência de conhecimentos e a eficácia do programa de conscientização, educação e treinamento.

Conscientização

Convém que um programa de conscientização sobre segurança da informação tenha como objetivo conscientizar o pessoal sobre suas responsabilidades pela segurança da informação e os meios pelos quais essas responsabilidades são cumpridas.

Convém que o programa de conscientização seja planejado de acordo com os papéis do pessoal na organização, incluindo pessoal interno e pessoal externo (por exemplo, consultores externos, fornecedores). Convém que as atividades no programa de conscientização sejam agendadas ao longo do tempo, preferencialmente regularmente, para que as atividades se repitam e abranjam pessoal novo. Convém que seja elaborado também com lições aprendidas dos incidentes de segurança da informação.

Convém que o programa de conscientização inclua uma série de atividades de conscientização através de canais físicos ou virtuais apropriados, como campanhas, folhetos, cartazes, boletins informativos, *websites*, sessões informativas, *briefings*, módulos de *e-learning* e *e-mails*.

Convém que a conscientização sobre a segurança da informação abranja aspectos gerais, como:

a) compromisso da direção com a segurança da informação em toda a organização;

b) necessidades de familiaridade e *compliance* em relação às regras e obrigações aplicáveis de segurança da informação, de acordo com a política de segurança da informação e as políticas específicas por tema, normas, leis, estatutos, regulamentos, contratos e acordos;

c) responsabilização do pessoal por suas próprias ações e omissões, e responsabilidades gerais para garantir ou proteger as informações pertencentes à organização e às partes interessadas;

d) procedimentos básicos de segurança da informação [por exemplo, relatórios de incidentes de segurança da informação (6.8)] e controles básicos [por exemplo, segurança de senhas (5.17)];

e) pontos de contato e recursos para informações adicionais e orientações sobre questões de segurança da informação, incluindo mais materiais de conscientização sobre segurança da informação.

Educação e treinamento

Convém que a organização identifique, prepare e implemente um plano de treinamento adequado para equipes técnicas cujos papéis requerem conjuntos de habilidades e conhecimentos específicos. Convém que as equipes técnicas tenham as habilidades para configurar e manter o nível de segurança necessário para dispositivos, sistemas, aplicações e serviços. Se houver habilidades ausentes, convém que a organização tome uma ação para adquiri-las.

Convém que o programa de educação e treinamento considere diferentes formas [por exemplo, palestras ou autoestudo, mentoria por especialistas ou consultores (treinamento *on-the-job*),

rotacionando os membros da equipe para acompanhar diferentes atividades, recrutando pessoas já qualificadas e contratando consultores]. O programa pode usar diferentes meios, incluindo ensino a distância, baseado na *web*, autoacelerado, entre outros. Convém que o pessoal técnico mantenha seus conhecimentos atualizados, assinando boletins informativos e revistas ou participando de conferências e eventos voltados ao aprimoramento técnico e profissional.

Outras informações

Ao compor um programa de conscientização, é importante não apenas focar no “o quê” e no “como”, mas também no “porquê”, quando possível. É importante que o pessoal entenda o objetivo da segurança da informação e o efeito potencial, positivo e negativo na organização, de seu próprio comportamento.

Conscientização, educação e treinamento em segurança da informação podem ser parte de, ou conduzidos em colaboração com, outras atividades, por exemplo, treinamento em gestão de informações, TIC, segurança, privacidade ou segurança.

6.4 Processo disciplinar

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger #Responder	#Segurança_em_ recursos_humanos	#Governança_e_ ecossistema

Controle

Convém que um processo disciplinar seja formalizado e comunicado, para tomar ações contra pessoal e outras partes interessadas relevantes que tenham cometido uma violação da política de segurança da informação.

Propósito

Assegurar que o pessoal e outras partes interessadas pertinentes entendam as consequências da violação da política de segurança da informação, para dissuadir e lidar adequadamente com as pessoas que cometeram a violação.

Orientação

Convém que o processo disciplinar não seja iniciado sem a confirmação prévia de que ocorreu uma violação da política de segurança da informação (ver 5.28).

Convém que o processo disciplinar formal forneça uma resposta categorizada, que considere fatores como:

a) a natureza (quem, o que quando, como) e gravidade da violação e suas consequências;

b) se o delito foi intencional (malicioso) ou não acidental (acidental);

c) se este é ou não um primeiro delito ou se é repetido;

d) se o infrator foi ou não devidamente treinado.

Convém que a resposta considere requisitos legais, estatutários, contratuais, regulamentares e comerciais relevantes, bem como outros fatores, conforme requerido. Convém que o processo disciplinar também seja usado como um impedimento para evitar que pessoal viole a política de segurança da informação, políticas específicas por tema e procedimentos para a segurança da informação. Violações deliberadas da política de segurança da informação podem requerer ações imediatas.

Outras informações

Convém que sempre que possível, a identidade dos indivíduos sujeitos a ações disciplinares seja protegida de acordo com os requisitos aplicáveis.

Quando os indivíduos demonstram um excelente comportamento em relação à segurança da informação, eles podem ser recompensados por promover a segurança da informação e incentivar o bom comportamento.

6.5 Responsabilidades após encerramento ou mudança da contratação

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Segurança_em_recursos_humanos #Gestão_de_ativos	#Governança_e_ecossistema

Controle

Convém que as responsabilidades e funções de segurança da informação que permaneçam válidos após o encerramento ou mudança da contratação sejam definidos, aplicados e comunicados ao pessoal e outras partes interessadas pertinentes.

Propósito

Proteger os interesses da organização como parte do processo de mudança ou encerramento da contratação ou de um contrato.

Orientação

Convém que processo de gestão da mudança ou encerramento da contratação defina quais responsabilidades e funções de segurança da informação convém permanecer válidos após a mudança ou encerramento. Isso pode incluir confidencialidade de informações, propriedade intelectual e outros conhecimentos obtidos, bem como responsabilidades contidas em qualquer outro acordo de confidencialidade (ver 6.6). Convém que as responsabilidades e funções ainda válidos após o encerramento da contratação ou do contrato estejam contidos nos contratos, acordos ou termos e condições de contratação (ver 6.2). Outros contratos ou acordos que permaneçam por um período definido após o encerramento da contratação do indivíduo também podem conter responsabilidades de segurança da informação.

Convém que as mudanças de responsabilidade ou de contratação sejam gerenciadas como o encerramento da contratação ou responsabilidade atual combinada com o início da nova responsabilidade ou contratação.

Convém que os papéis e responsabilidades de segurança da informação de qualquer indivíduo que sai ou muda de papel sejam identificadas e transferidas para outro indivíduo.

Convém que seja estabelecido um processo para a comunicação das mudanças e dos procedimentos operacionais ao pessoal, demais partes interessadas e pessoas de contato pertinentes (por exemplo, aos clientes e fornecedores).

Convém que o processo de encerramento ou mudança da contratação também seja aplicado ao pessoal externo (ou seja, fornecedores) quando ocorre encerramento de contratação, o término de um contrato ou o término de um trabalho com a organização, ou quando houver uma mudança de trabalho dentro da organização.

Outras informações

Em muitas organizações, a função de recursos humanos é comumente responsável por todo o processo de encerramento da contratação e trabalha em conjunto com o gestor da pessoa em transição para gerenciar os aspectos de segurança da informação dos procedimentos relevantes. No caso de um prestador de serviço fornecido por uma parte externa (por exemplo, através de um fornecedor), esse processo de encerramento é realizado pela parte externa de acordo com o contrato entre a organização e a parte externa.

6.6 Acordos de confidencialidade ou não divulgação

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Segurança_em_recursos_humanos #Proteção_da_informação #Segurança_nas_relações_com_fornecedores	#Governança_e_ecossistema

Controle

Convém que acordos de confidencialidade ou não divulgação que reflitam as necessidades da organização para a proteção das informações sejam identificados, documentados, analisados criticamente em intervalos regulares e assinados por pessoal e outras partes interessadas pertinentes.

Propósito

Manter a confidencialidade das informações acessíveis pelo pessoal ou por partes externas.

Orientação

Convém que acordos de confidencialidade ou não divulgação abordem a exigência de proteger informações confidenciais usando termos legalmente aplicáveis. Acordos de confidencialidade ou não divulgação são aplicáveis as partes interessadas e ao pessoal da organização. Com base nos requisitos de segurança da informação de uma organização, convém que os termos dos acordos sejam determinados levando em consideração o tipo de informação que será manuseada, seu nível de classificação, seu uso e o acesso permitido pela outra parte. Para identificar os requisitos para acordos de confidencialidade ou não divulgação, convém que sejam considerados os seguintes elementos:

a) uma definição das informações a serem protegidas (por exemplo, informações confidenciais);

b) a duração esperada de um acordo, incluindo casos em que a confidencialidade pode ser mantida indefinidamente ou até que as informações se tornam publicamente disponíveis;

c) as ações necessárias quando um acordo é rescindido;

d) as responsabilidades e ações dos signatários para evitar a divulgação de informações não autorizadas;

e) a propriedade de informações, segredos comerciais e propriedade intelectual, e como isso se relaciona com a proteção de informações confidenciais;

f) o uso permitido da informação confidencial e direitos do signatário para o uso da informação;

g) o direito de auditar e monitorar atividades que envolvam informações confidenciais para circunstâncias altamente sensíveis;

h) o processo de notificação e emissão de relatórios de divulgação não autorizada ou vazamento de informações confidenciais;

i) os termos para que as informações sejam devolvidas ou destruídas no término do acordo;

j) as ações esperadas a serem tomadas no caso de não conformidade com o acordo.

Convém que a organização considere a conformidade dos acordos de confidencialidade e não divulgação com a jurisdição para a qual eles se aplicam (ver 5.31, 5.32, 5.33, 5.34).

Convém que os requisitos para acordos de confidencialidade e não divulgação sejam analisados criticamente, de forma periódica, e quando ocorrem mudanças que influenciem esses requisitos.

Outras informações

Acordos de confidencialidade e não divulgação protegem as informações da organização e informam aos signatários de sua responsabilidade de proteger, usar e divulgar informações de forma responsável e autorizada.

6.7 Trabalho remoto

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo #Corretivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Gestão_de_ativos #Proteção_da_informação #Segurança_fisica #Segurança_de_ sistemas_e_ rede	#Proteção

Controle

Convém que medidas de segurança sejam implementadas quando as pessoas estiverem trabalhando remotamente para proteger as informações acessadas, tratadas ou armazenadas fora das instalações da organização.

Propósito

Assegurar a segurança das informações quando o pessoal estiver trabalhando remotamente.

Orientação

O trabalho remoto ocorre sempre que o pessoal da organização trabalha em um local fora das instalações da organização, acessando informações seja em cópias impressas ou eletronicamente via equipamento de TIC. Os ambientes de trabalho remoto incluem aqueles chamados de “trabalho remoto”, “teletrabalho”, “local de trabalho flexível”, “ambientes de trabalho virtuais” e “manutenção remota”.

NOTA É possível que nem todas as recomendações nesta orientação possam ser aplicadas em razão de regulamentações e legislação locais e em diferentes jurisdições.

Convém que as organizações que permitem atividades de trabalho remotas emitam uma política específica por tema sobre trabalho remoto que define as condições e restrições pertinentes. Convém que, se julgar aplicável, sejam consideradas as seguintes questões:

a) a segurança física existente ou proposta no local de trabalho remoto, levando em conta a segurança física do prédio e o ambiente local, incluindo as diferentes jurisdições legais onde o pessoal está localizado;

b) as regras e os mecanismos de segurança para o ambiente físico remoto, como armários trancados de arquivos, transporte seguro entre locais e regras para acesso remoto, mesa limpa, impressão e descarte de informações e outros ativos associados e relatórios de eventos de segurança da informação (ver 6.8);

c) os ambientes de trabalho físicos remotos esperados;

d) os requisitos de segurança das comunicações, levando em conta a necessidade de acesso remoto aos sistemas da organização, a sensibilidade das informações a serem acessadas e trafegadas sobre o *link* de comunicação e a sensibilidade dos sistemas e aplicações;

e) o uso de acesso remoto, como acesso a “*desktop* virtual”, que estabelece o tratamento e armazenamento adequado de informações em equipamentos de propriedade particular;

f) a ameaça de acesso não autorizado a informações ou recursos de outras pessoas no local de trabalho remoto (por exemplo, família e amigos);

g) a ameaça de acesso não autorizado a informações ou recursos de outras pessoas em locais públicos;

h) o uso de redes domésticas e redes públicas, e requisitos ou restrições na configuração de serviços de rede sem fio;

i) uso de medidas de segurança, como *firewalls* e proteção contra *malware*;

j) os mecanismos seguros para implantação e inicialização de sistemas remotamente;

k) os mecanismos seguros de autenticação e habilitação de privilégios de acesso de acordo com a vulnerabilidade de mecanismos de autenticação de fator único onde o acesso remoto à rede da organização é permitido.

Convém que as diretrizes e medidas a serem consideradas incluam:

a) o fornecimento de equipamentos adequados e móveis de armazenamento para as atividades de trabalho remoto, onde a utilização de equipamentos de propriedade particular que não estão sob o controle da organização não é permitida;

b) uma definição do trabalho permitido, a classificação das informações que podem ser mantidas e os sistemas e serviços internos que o trabalhador remoto está autorizado a acessar;

c) a provisão de treinamento para aqueles que trabalham remotamente e aqueles que fornecem suporte. Convém que isso inclua como conduzir negócios de forma segura enquanto trabalha remotamente;

d) a provisão de equipamentos de comunicação adequados, incluindo métodos para garantir acesso remoto, como requisitos de bloqueios de tela do dispositivo e temporizadores de inatividade; a habilitação do rastreamento de localização do dispositivo; instalação de recursos para limpeza remota (“*wipe*”);

e) a segurança física;

f) as regras e orientações sobre o acesso de familiares e visitantes ao equipamento e à informação;

g) a provisão de suporte e manutenção de *hardware* e *software*;

h) a provisão de seguro;

i) os procedimentos para *backup* e continuidade do negócio;

j) a auditoria e o monitoramento da segurança;

k) a revogação de autoridade e direitos de acesso e devolução do equipamento quando as atividades do trabalho remoto são encerradas.

Outras informações

Não há outra informação.

6.8 Relato de eventos de segurança da informação

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Detectivo	#Confidencialidade #Integridade #Disponibilidade	#Detectar	#Gestão_de_eventos_de_segurança_da_informação	#Defesa

Controle

Convém que a organização forneça um mecanismo para que as pessoas relatem eventos de segurança da informação observados ou suspeitos através de canais apropriados em tempo hábil.

Propósito

Oferecer apoio em tempo hábil a relatos, consistentes e eficazes de eventos de segurança da informação que podem ser identificados pelo pessoal.

Orientação

Convém que todo o pessoal e os usuários estejam conscientes de suas responsabilidades de relatar eventos de segurança da informação o mais rápido possível, a fim de prevenir ou minimizar o efeito dos incidentes de segurança da informação.

Convém que eles também estejam cientes do procedimento de relato de eventos de segurança da informação e do ponto de contato para o qual convém que os eventos sejam relatados. Convém que o mecanismo de relato seja o mais fácil, acessível e disponível possível. Eventos de segurança da informação incluem incidentes, violações e vulnerabilidades.

As situações a serem consideradas para relato de eventos de segurança da informação incluem:

a) controles de segurança da informação ineficazes;

b) violação das expectativas de confidencialidade, integridade ou disponibilidade das informações;

c) erros humanos;

d) não *compliance* com a política de segurança da informação, políticas específicas por tema ou normas aplicáveis;

e) violações de procedimentos de segurança física;

f) mudanças de sistema que não passaram pelo processo de gestão de mudanças;

g) defeitos ou outro comportamento anômalo do sistema de *software* ou *hardware*;

h) violações de acesso;

i) vulnerabilidades;

j) suspeita de infecção por *malware*.

Convém que o pessoal e os usuários sejam aconselhados a não tentar provar suspeitas de vulnerabilidades de segurança da informação. Testar vulnerabilidades pode ser interpretado como um potencial uso indevido do sistema e também pode causar danos ao sistema de informações ou serviço, podendo corromper ou tornar incompreensível as evidências digitais. Em última análise, isso pode resultar em responsabilidade legal para o indivíduo que realiza o teste.

Outras informações

Ver a série ISO/IEC 27035 para obter informações adicionais.

7 Controles físicos

7.1 Perímetros de segurança física

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Segurança_fisica	#Proteção

Controle

Convém que perímetros de segurança sejam definidos e usados para proteger áreas que contenham informações e outros ativos associados.

Propósito

Evitar acesso físico não autorizado, danos e interferências nas informações da organização e outros ativos associados.

Orientação

Convém que as seguintes diretrizes sejam consideradas e implementadas, quando apropriado, para perímetros de segurança física:

a) definir perímetros de segurança e a localização e resistência de cada um dos perímetros de acordo com os requisitos de segurança da informação relacionados aos ativos dentro do perímetro;

b) ter perímetros fisicamente sólidos para um edifício ou local contendo instalações de tratamento da informação (ou seja, convém que não haja lacunas no perímetro ou áreas onde um arrombamento pode ocorrer facilmente). Convém que os telhados externos, paredes, tetos e pisos do local sejam de construção sólida e todas as portas externas sejam adequadamente protegidas contra acesso não autorizado por meio de mecanismos de controle (por exemplo, barras, alarmes, fechaduras). Convém que portas e janelas sejam trancadas quando estiverem sem monitoração e uma proteção externa seja considerada para janelas, particularmente no andar térreo; convém que os pontos de ventilação também sejam considerados;

c) alarmar, monitorar e testar todas as portas de incêndio do perímetro de segurança, em conjunto com as paredes, para estabelecer o nível de resistência requerido, de acordo com as normas adequadas. Convém que eles operem no modo à prova de falhas.

Outras informações

Proteção física pode ser alcançada criando uma ou mais barreiras físicas em torno das instalações da organização e dos recursos de tratamento da informação.

Uma área segura pode ser um escritório trancável ou várias salas cercadas por uma barreira interna contínua de segurança física. Barreiras adicionais e perímetros para controlar o acesso físico podem ser necessários entre áreas com diferentes requisitos de segurança dentro do perímetro de segurança. Convém que a organização considere ter medidas de segurança física que possam ser reforçadas durante o aumento de situações de ameaça.

7.2 Entrada física

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Segurança_física #Gestão_de_identidade_e_acesso	#Proteção

Controle

Convém que as áreas seguras sejam protegidas por controles de entrada e pontos de acesso apropriados.

Propósito

Assegurar que ocorra apenas acesso físico autorizado às informações da organização e outros ativos associados.

Orientação

Geral

Convém que os pontos de acesso, como áreas de entrega e carregamento e outros pontos onde pessoas não autorizadas podem entrar nas instalações, sejam controlados e, se possível, isolados dos recursos de tratamento da informação, para evitar acesso não autorizado.

Convém que as seguintes diretrizes sejam consideradas:

a) restringir o acesso aos locais e edifícios apenas ao pessoal autorizado. Convém que o processo de gestão dos direitos de acesso às áreas físicas inclua o fornecimento, análise crítica periódica, atualização e revogação das autorizações (ver 5.18);

b) manter e monitorar de forma segura um livro de registro físico ou trilha de auditoria eletrônica de todos os acessos e proteger todos os registros (ver 5.33) e informações de autenticação sensíveis;

c) estabelecer e implementar um processo e mecanismos técnicos para a gestão do acesso às áreas onde a informação é tratada ou armazenada. Os mecanismos de autenticação incluem o uso de cartões de acesso, biometria ou autenticação de dois fatores, como um cartão de acesso e PIN secreto. Convém que sejam consideradas portas duplas de segurança para acesso a áreas sensíveis;

d) implantar uma área de recepção monitorada pelo pessoal ou outros meios para controlar o acesso físico ao local ou edifício;

e) inspecionar e examinar pertences pessoais do pessoal e partes interessadas no momento da entrada e saída;

NOTA Podem existir legislação e regulamentos locais relacionados à possibilidade de inspeção de pertences pessoais.

f) requerer que todo o pessoal e as partes interessadas usem algum tipo visível de identificação e notifiquem imediatamente o pessoal de segurança se encontrarem visitantes não acompanhados e qualquer pessoa que não esteja usando uma identificação visível. Convém que crachás facilmente distinguíveis sejam considerados para melhor identificar funcionários permanentes, fornecedores e visitantes;

g) conceder acesso restrito ao pessoal do fornecedor a áreas seguras ou recursos de tratamento da informação apenas quando necessário. Convém que esse acesso seja autorizado e monitorado;

h) dar atenção especial à segurança de acesso físico no caso de edifícios que detêm ativos para várias organizações;

i) elaborar medidas de segurança física que possam ser reforçadas quando a probabilidade de incidentes físicos aumentar;

j) proteger outros pontos de entrada contra acesso não autorizado, como saídas de emergência;

k) implantar um processo de gerenciamento chave para assegurar o gerenciamento das chaves físicas ou informações de autenticação (por exemplo, códigos de bloqueio, fechaduras de combinação para escritórios, salas e instalações, como armários de chaves) e para assegurar um livro de registro ou auditoria anual de chaves e que o acesso para as chaves físicas ou informações de autenticação seja controlado (ver 5.17 para obter mais orientações sobre informações de autenticação).

Visitantes

Convém que sejam consideradas as seguintes diretrizes:

a) autenticar a identidade dos visitantes por meios apropriados;

b) registrar a data e a hora de entrada e saída dos visitantes;

c) permitir o acesso apenas para visitantes para fins específicos e autorizados e com instruções sobre os requisitos de segurança da área e procedimentos de emergência;

d) supervisionar todos os visitantes, a menos que uma exceção explícita seja concedida.

Áreas de entrega e carregamento e material de entrada

Convém que sejam consideradas as seguintes diretrizes:

a) restringir o acesso a áreas de entrega e carregamento da área exterior do prédio para o pessoal identificado e autorizado;

b) projetar as áreas de entrega e carregamento para que as entregas possam ser carregadas e descarregadas sem que o entregador obtenha acesso não autorizado a outras partes do edifício;

c) proteger as portas externas das áreas de entrega e carregamento quando as portas para as áreas restritas são abertas;

d) inspecionar e examinar as entregas recebidas para detecção de explosivos, produtos químicos ou outros materiais perigosos antes de serem transportados de áreas de entrega e carregamento;

e) registrar as entregas recebidas de acordo com os procedimentos de gestão de ativos (ver 5.9 e 7.10) quando da sua entrada no local;

f) segregar fisicamente remessas de entrada e saída, sempre que possível;

g) inspecionar materiais recebidos para evidenciar adulteração no caminho. Se a adulteração for descoberta, convém que ela seja imediatamente reportada ao pessoal da segurança.

Outras informações

Não há outra informação.

7.3 Segurança de escritórios, salas e instalações

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Segurança_física #Gestão_de_ativos	#Proteção

Controle

Convém que seja projetada e implementada segurança física para escritórios, salas e instalações.

Propósito

Evitar acesso físico não autorizado, danos e interferências nas informações da organização e outros ativos associados em escritórios, salas e instalações.

Orientação

Convém que as seguintes diretrizes sejam consideradas para proteger escritórios, salas e instalações:

a) instalações-chave localizadas de maneira a evitar o acesso do público;

b) quando aplicável, assegurar que os edifícios sejam discretos e dar indicação mínima de seu propósito, sem letreiros evidentes, fora ou dentro do edifício, identificando a presença de atividades de tratamento de informações;

c) projetar as instalações para evitar que informações ou atividades confidenciais sejam visíveis e possam ser ouvidas da parte externa. Convém que a blindagem eletromagnética seja considerada conforme apropriado;

d) não tornar listas de pessoas, guias telefônicos internos e mapas acessíveis *on-line* identificando locais de instalações de tratamento de informações confidenciais facilmente acessíveis para qualquer pessoa não autorizada.

Outras informações

Não há outra informação.

7.4 Monitoramento de segurança física

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo #Detectivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger #Detectar	#Segurança_física	#Proteção #Defesa

Controle

Convém que as instalações sejam monitoradas continuamente para acesso físico não autorizado.

Propósito

Detectar e impedir o acesso físico não autorizado.

Orientação

Convém que as instalações físicas sejam monitoradas por sistemas de vigilância, que podem incluir guardas, alarmes de intrusos, sistemas de videomonitoramento, como de circuito fechado de TV e *software* de gerenciamento de informações de segurança física, gerenciados internamente ou por um provedor de serviços de monitoramento.

Convém que o acesso a edifícios que abrigam sistemas críticos seja monitorado continuamente para detectar acesso não autorizado ou comportamento suspeito por:

a) instalação de sistemas de videomonitoramento, como circuito fechado de TV, para visualizar e registrar acesso a áreas sensíveis dentro e fora das instalações de uma organização;

b) instalação, de acordo com as normas aplicáveis pertinentes, e testes periódicos de contato, de som ou detectores de movimento para acionar um alarme de intrusão como:

   1) instalação de detectores de contato que acionam um alarme quando um contato é feito ou quebrado em qualquer lugar onde um contato possa ser feito ou quebrado (como janelas e portas e debaixo de objetos) para ser usado como alarme de pânico;

   2) detectores de movimento baseados na tecnologia infravermelho que acionam um alarme quando um objeto passa pelo seu campo de visão;

   3) instalação de sensores sensíveis ao som de vidro quebrando, que podem ser usados para acionar um alarme para alertar o pessoal de segurança;

c) uso desses alarmes para cobrir todas as portas externas e janelas acessíveis. Convém que áreas desocupadas fiquem alarmadas o tempo todo; convém que a cobertura também seja fornecida para outras áreas (por exemplo, computador ou salas de comunicação).

Convém que o projeto dos sistemas de monitoramento seja mantido em sigilo porque a divulgação pode facilitar arrombamentos não detectados.

Convém que os sistemas de monitoramento sejam protegidos contra acesso não autorizado, a fim de evitar que informações de vigilância, como *feeds* de vídeo, sejam acessadas por pessoas não autorizadas ou sistemas sejam desativados remotamente.

Convém que o painel de controle do sistema de alarme seja colocado em uma zona alarmada e, para alarmes de segurança, em um lugar que permite uma rota de saída fácil para a pessoa que define o alarme. Convém que o painel de controle e os detectores tenham mecanismos à prova de adulteração. Convém que o sistema seja testado regularmente para garantir que esteja funcionando como planejado, especialmente se seus componentes forem alimentados por bateria.

Convém que qualquer mecanismo de monitoramento e gravação seja usado levando em consideração as leis e regulamentos locais, incluindo a legislação de proteção de dados e proteção de DP, especialmente em relação ao monitoramento de pessoal e períodos de retenção de vídeo gravados.

Outras informações

Não há outra informação.

7.5 Proteção contra ameaças físicas e ambientais

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Segurança_física	#Proteção

Controle

Convém que a proteção contra ameaças físicas e ambientais, como desastres naturais e outras ameaças físicas intencionais ou não intencionais à infraestrutura, seja projetada e implementada.

Propósito

Prevenir ou reduzir as consequências de eventos originários de ameaças físicas e ambientais.

Orientação

Convém que processos de avaliação de risco para identificar as potenciais consequências das ameaças físicas e ambientais sejam realizadas antes do início das operações críticas em um local físico e em intervalos regulares. Convém que as salvaguardas necessárias sejam implementadas e as mudanças nas ameaças sejam monitoradas. Convém que sejam obtidos conselhos especializados sobre como gerenciar riscos decorrentes de ameaças físicas e ambientais, como incêndio, inundação, terremoto, explosão, manifestação civil, resíduos tóxicos, emissões ambientais e outras formas de desastres naturais ou desastres causados por seres humanos.

Convém que a localização e construção de instalações físicas considerem:

a) a topografia local, como elevação apropriada, cursos de água e linhas de falha tectônica;

b) as ameaças urbanas, como locais com alto perfil para atrair manifestação política, atividade criminosa ou ataques terroristas.

Convém que com base nos resultados do processo avaliação de riscos, sejam identificadas ameaças físicas e ambientais relevantes e controles apropriados considerados nos seguintes contextos como exemplos:

a) fogo: instalação e configuração de sistemas capazes de detectar incêndios em um estágio inicial para enviar alarmes ou acionar sistemas de supressão de incêndio, a fim de evitar danos causados pelo fogo à mídia de armazenamento e a sistemas de tratamento de informações relacionados. Convém que a supressão do fogo seja realizada utilizando a substância mais apropriada no que diz respeito ao ambiente circundante (por exemplo, gás em espaços confinados);

b) inundações: instalação de sistemas capazes de detectar inundações em um estágio inicial sob os andares de áreas que contêm mídia de armazenamento ou sistemas de tratamento de informações. Convém que bombas de água ou meios equivalentes sejam prontamente disponibilizadas no caso de inundações;

c) sobrecargas elétricas: adotar sistemas capazes de proteger sistemas de informação de servidores e clientes contra sobrecargas elétricas ou eventos semelhantes para minimizar as consequências de tais eventos;

d) explosivos e armas: realizar inspeções aleatórias para a presença de explosivos ou armas em pessoal, veículos ou mercadorias que entram nas instalações de tratamento de informações sensíveis.

Outras informações

Cofres ou outras formas de instalações de armazenamento seguras podem proteger as informações armazenadas contra desastres como fogo, terremoto, inundação ou explosão.

As organizações podem considerar os conceitos de prevenção ao crime por meio de projetos ambientais ao projetar os controles para proteger seu meio ambiente e reduzir as ameaças urbanas. Por exemplo, em vez de usar postes de amarração (*bollards*), estátuas ou recursos de água podem servir como um detalhe e uma barreira física.

7.6 Trabalho em áreas seguras

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Segurança_física	#Proteção

Controle

Convém que medidas de segurança para trabalhar em áreas seguras sejam projetadas e implementadas.

Propósito

Proteger as informações e outros ativos associados em áreas seguras contra danos e interferência não autorizada do pessoal que trabalha nessas áreas.

Orientação

Convém que as medidas de segurança para trabalhar em áreas seguras sejam aplicadas a todo o pessoal e abranjam todas as atividades ocorrendo na área segura.

Convém que sejam consideradas as seguintes diretrizes:

a) conscientizar o pessoal apenas sobre a existência ou atividades dentro de uma área segura baseado na necessidade de saber;

b) evitar trabalhos não supervisionados em áreas seguras, tanto por razões de segurança quanto para reduzir as chances de atividades maliciosas;

c) bloqueio físico e inspeção periódica de áreas seguras vagas;

d) não permitir equipamentos fotográficos, de vídeo, áudio ou de gravação, como câmeras em dispositivos *endpoint* do usuário, a menos que autorizados;

e) controlar adequadamente o transporte e o uso de dispositivos *endpoint* do usuário em áreas seguras;

f) postar procedimentos de emergência de forma facilmente visível ou acessível.

Outras informações

Não há outra informação.

7.7 Mesa limpa e tela limpa

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade	#Proteger	#Segurança_física	#Proteção

Controle

Convém que regras de mesa limpa para documentos impressos e mídia de armazenamento removível e regras de tela limpa para os recursos de tratamento das informações sejam definidas e adequadamente aplicadas.

Propósito

Reduzir os riscos de acesso não autorizado, perda e danos às informações em mesas, telas e em outros locais acessíveis durante e fora do horário comercial.

Orientação

Convém que a organização estabeleça e comunique uma política específica por tema sobre mesa limpa e tela limpa para todas as partes interessadas relevantes.

Convém que as seguintes diretrizes sejam consideradas:

a) bloquear informações de negócios sensíveis ou críticas (por exemplo, em papel ou em mídia de armazenamento eletrônico) (idealmente em um cofre, gabinete ou outra forma de mobiliário de segurança) quando não mais requerida, especialmente quando o escritório estiver desocupado;

b) proteger os dispositivos *endpoint* do usuário através de cadeados ou outros meios de segurança quando não estiver em uso ou sem vigilância;

c) encerrar sessões nos dispositivos *endpoint* do usuário ou proteger por um mecanismo de bloqueio de tela e de teclado, controlado por um mecanismo de autenticação do usuário quando sem supervisão. Convém que os computadores e sistemas sejam configurados com um recurso de tempo-limite ou encerramento de sessão automáticos;

d) fazer com que o autor colete saídas de impressoras ou multifuncionais imediatamente. Usar impressoras com uma função de autenticação, de modo que os autores são os únicos que podem obter suas impressões e somente quando estão ao lado da impressora;

e) armazenar de forma segura documentos e mídia de armazenamento removível contendo informações confidenciais e, quando não for mais necessário, descartá-los usando mecanismos de descarte seguro;

f) estabelecer e comunicar regras e orientações para a configuração de alertas nas telas (por exemplo, desligar os novos alertas de *e-mail* e mensagens, se possível, durante apresentações, compartilhamento de tela ou em área pública);

g) limpar informações confidenciais ou críticas em quadros brancos e outros tipos de recursos de exibição quando não for mais necessário.

Convém que a organização tenha procedimentos em vigor ao desocupar instalações, incluindo a realização de uma varredura final antes de sair, para assegurar que os ativos da organização não sejam deixados para trás (por exemplo, documentos que estão atrás de gavetas ou mobílias).

Outras informações

Não há outra informação.

7.8 Localização e proteção de equipamentos

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Segurança_física #Gestão_de_ativos	#Proteção

Controle

Convém que os equipamentos sejam posicionados com segurança e proteção.

Propósito

Reduzir os riscos de ameaças físicas e ambientais, e de acesso não autorizado e danos.

Orientação

Convém que as seguintes diretrizes sejam consideradas para proteger os equipamentos:

a) posicionar os equipamentos de modo a minimizar o acesso desnecessário às áreas de trabalho e evitar acesso não autorizado;

b) posicionar cuidadosamente os recursos de tratamento de informações que lidam com dados confidenciais, para reduzir o risco de informações serem visualizadas por pessoas não autorizadas durante seu uso;

c) adotar controles para minimizar o risco de potenciais ameaças físicas e ambientais [por exemplo, roubo, incêndio, explosivos, fumaça, água (ou falha no fornecimento de água), poeira, vibração, efeitos químicos, interferência de fornecimento elétrico, interferência nas comunicações, radiação eletromagnética e vandalismo];

d) estabelecer diretrizes sobre comer, beber e fumar nas proximidades das instalações de tratamento de informações;

e) monitorar condições ambientais, como temperatura e umidade, para condições que possam afetar negativamente o funcionamento de instalações de tratamento de informações;

f) aplicar proteção contra raios em todos as edificações e instalar filtros de proteção contra raios em todas as linhas de entrada de energia e comunicação;

g) considerar o uso de métodos de proteção especial, como teclado de membranas, para equipamentos em ambientes industriais;

h) proteger equipamentos que tratam informações confidenciais para minimizar o risco de vazamento de informações devido à emanação eletromagnética;

i) separação física das instalações de tratamento de informações gerenciadas pela organização daquelas que não são gerenciadas pela organização.

Outras informações

Não há outra informação.

7.9 Segurança de ativos fora das instalações da organização

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Segurança_física #Gestão_de_ativos	#Proteção

Controle

Convém proteger os ativos fora das instalações da organização.

Propósito

Evitar perdas, danos, roubos ou comprometimento de ativos fora das instalações da organização e interrupção da operação da organização.

Orientação

Qualquer dispositivo usado fora das instalações da organização que armazene ou trate informações (por exemplo, dispositivo móvel), incluindo dispositivos pertencentes à organização e dispositivos de

propriedade privada e usados em nome da organização (BYOD) necessita estar protegido. Convém que o uso desses dispositivos seja autorizado pela direção.

Convém que sejam consideradas as seguintes diretrizes para a proteção de equipamentos que armazenam ou tratam informações fora das instalações da organização:

a) não deixar sem vigilância os equipamentos e meios de armazenamento retirados das instalações da organização, em locais públicos e inseguros;

b) observar as instruções dos fabricantes para proteger os equipamentos o tempo todo (por exemplo, proteção contra exposição a fortes campos eletromagnéticos, água, calor, umidade, poeira);

c) quando equipamentos fora das instalações forem transferidos entre diferentes indivíduos ou partes interessadas, manter um registro que defina a cadeia de custódia dos equipamentos, incluindo pelo menos nomes e organizações dos responsáveis pelo equipamento. Convém que as informações que não precisam ser transferidas com o ativo sejam excluídas com segurança antes da transferência;

d) quando necessário e possível, exigir autorização para que equipamentos e mídias sejam removidos das instalações da organização e manter um registro dessas remoções a fim de manter uma trilha de auditoria (ver 5.14);

e) proteger contra a visualização de informações no dispositivo (por exemplo, celular ou *laptop*) no transporte público, e os riscos associados a espiar por cima dos ombros;

f) implementar o rastreamento de localização e a capacidade de limpeza remota de dispositivos.

A instalação permanente de equipamentos fora das instalações da organização [como antenas e caixas eletrônicos (ATM)] pode estar sujeita ao risco de danos, roubo ou espionagem. Esses riscos podem variar consideravelmente entre os locais e convém que sejam levados em conta na determinação das medidas mais adequadas. Convém que as seguintes diretrizes sejam consideradas ao posicionar este equipamento fora das instalações da organização:

a) monitoramento de segurança física (ver 7.4);

b) proteção contra ameaças físicas e ambientais (ver 7.5);

c) controles de acesso físico e à prova de adulteração;

d) controles de acesso lógicos.

Outras informações

Mais informações sobre outros aspectos da proteção de equipamentos de armazenamento e tratamento de informações e dispositivos *endpoint* do usuário final podem ser encontradas em 8.1 e 6.7.

7.10 Mídia de armazenamento

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Segurança_física #Gestão_de_ativos	#Proteção

Controle

Convém que as mídias de armazenamento sejam gerenciadas por seu ciclo de vida de aquisição, uso, transporte e descarte, de acordo com o esquema de classificação e com os requisitos de manuseio da organização.

Propósito

Assegurar a divulgação, modificação, remoção ou destruição de informações apenas de forma autorizada sobre as mídias de armazenamento.

Orientação

Mídia de armazenamento removível

Convém que sejam consideradas as seguintes diretrizes para o gerenciamento de mídias de armazenamento removíveis:

a) estabelecer uma política específica por tema sobre o gerenciamento de mídia de armazenamento removível e comunicar essa política específica por tema para qualquer pessoa que use ou manuseie mídia de armazenamento removível;

b) quando necessário e possível, exigir autorização para que os meios de armazenamento sejam removidos da organização e manter um registro dessas remoções, a fim de manter uma trilha de auditoria;

c) armazenar todas as mídias de armazenamento em um ambiente seguro e protegido de acordo com a classificação de suas informações e protegê-las contra ameaças ambientais (como calor, umidade, ambiente úmido, campo eletrônico ou envelhecimento), de acordo com as especificações dos fabricantes;

d) usar técnicas criptográficas para proteger informações nas mídias de armazenamento removíveis, se a confidencialidade ou a integridade das informações forem considerações importantes;

e) mitigar o risco de degradação de mídia de armazenamento, enquanto as informações armazenadas ainda forem necessárias, transferindo as informações para novas mídias de armazenamento antes de se tornarem ilegíveis;

f) armazenar múltiplas cópias de informações de grande valor, em mídias de armazenamento separadas, para reduzir ainda mais o risco de dano ou perda de informações coincidentes;

g) considerar o registro das mídias de armazenamento removível para limitar a chance de perda de informações;

h) somente habilitar as portas de mídia de armazenamento removíveis (por exemplo, *slots* de cartão SD e portas USB) se houver uma razão organizacional para seu uso;

i) monitorar a transferência de informações para mídia de armazenamento removível, onde houver a necessidade de usar tais meios de armazenamento;

j) informações podem ser vulneráveis a acesso não autorizado, uso indevido ou alteração indevida durante o transporte físico, por exemplo, ao enviar mídia de armazenamento pelos serviços postais ou por mensageiros.

Neste controle, a mídia inclui documentos em papel. Ao transferir a mídia de armazenamento físico, aplicar as medidas de segurança de 5.14.

Reutilização ou descarte seguro

Convém que os procedimentos para a reutilização ou descarte seguro de mídia de armazenamento sejam estabelecidos para minimizar o risco de vazamento de informações confidenciais a pessoas não autorizadas. Convém que os procedimentos de reutilização ou descarte seguro de meios de armazenamento contendo informações confidenciais sejam proporcionais à sensibilidade dessas informações. Convém que os seguintes itens sejam considerados:

a) se as mídias de armazenamento contendo informações confidenciais precisarem ser reutilizadas dentro da organização, excluir os dados com segurança ou formatar a mídia de armazenamento antes de reutilizar (ver 8.10);

b) descartar de forma segura a mídia de armazenamento contendo informações confidenciais, quando não forem mais necessárias (por exemplo, destruindo, triturando ou excluindo o conteúdo com segurança);

c) ter procedimentos implementados para identificar os itens que podem exigir descarte seguro;

d) muitas organizações oferecem serviços de coleta e descarte para mídia de armazenamento. Convém tomar o devido cuidado na seleção de um fornecedor externo apropriado com controles e experiência adequados;

e) registrar o descarte de itens sensíveis, a fim de manter uma trilha de auditoria;

f) ao acumular mídia de armazenamento para descarte, considerar o efeito de agregação, que pode fazer com que uma grande quantidade de informações não sensíveis se torne sensível.

Convém que um processo de avaliação de risco seja realizado em dispositivos danificados contendo dados sensíveis, para determinar se convém que os itens sejam fisicamente destruídos em vez de enviados para reparo ou descartados (ver 7.14).

Outras informações

Quando as informações confidenciais na mídia de armazenamento não forem criptografadas, convém considerar proteção física adicional na mídia de armazenamento.

7.11 Serviços de infraestrutura

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo #Detectivo	#Integridade #Disponibilidade	#Proteger #Detectar	#Segurança_física	#Proteção

Controle

Convém que as instalações de tratamento de informações sejam protegidas contra falhas de energia e outras disrupções causadas por falhas nos serviços de infraestrutura.

Propósito

Evitar perdas, danos ou comprometimento de informações e outros ativos associados, ou a interrupção das operações da organização devido à falha e disrupção nos serviços de infraestrutura.

Orientação

As organizações dependem de serviços de infraestrutura (por exemplo, energia elétrica, telecomunicações, abastecimento de água, gás, esgoto, ventilação e ar-condicionado) para apoiar suas instalações de tratamento de informações. Portanto, convém à organização:

a) assegurar que os equipamentos que apoiam o serviço de infraestrutura sejam configurados, operados e mantidos de acordo com as especificações do fabricante pertinente;

b) assegurar que os serviços de infraestrutura sejam avaliados regularmente frente à sua capacidade de atender ao crescimento dos negócios e interações com outros serviços de infraestrutura;

c) assegurar que os equipamentos que apoiam os serviços de infraestrutura sejam inspecionados e testados regularmente para assegurar seu bom funcionamento;

d) se necessário, acionar alarmes para detectar falhas na infraestrutura;

e) se necessário, assegurar que a infraestrutura tenha múltiplas fontes com roteamento físico diversificado;

f) assegurar que os equipamentos dos serviços de infraestrutura estejam em uma rede separada dos recursos de tratamento de informações, caso conectados a uma rede;

g) assegurar que os equipamentos que suportam os serviços de infraestrutura estejam conectados à *internet* apenas quando necessário e somente de maneira segura.

Convém que iluminação e comunicação de emergência sejam fornecidas. Convém que interruptores e válvulas de emergência para cortar energia, água, gás ou outras utilidades estejam localizados perto de saídas de emergência ou em salas de equipamentos. Convém que os detalhes de contato de emergência sejam registrados e disponibilizados para o pessoal em caso de paralisação.

Outras informações

Redundância adicional para conectividade de rede pode ser obtida por meio de múltiplas rotas com uso de mais um provedor de serviços de infraestrutura.

7.12 Segurança do cabeamento

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Disponibilidade	#Proteger	#Segurança_física	#Proteção

Controle

Convém que os cabos que transportam energia ou dados ou que sustentam serviços de informação sejam protegidos contra interceptação, interferência ou danos.

Propósito

Evitar perdas, danos, roubo ou comprometimento de informações e outros ativos associados à interrupção das operações da organização relacionadas ao cabeamento de energia e de comunicação.

Orientação

Convém que sejam consideradas as seguintes diretrizes para a segurança do cabeamento:

a) linhas de energia e telecomunicação em instalações de tratamento de informações sejam subterrâneas sempre que possível, ou sujeitas à proteção alternativa adequada, como protetor de cabos de piso e poste; se os cabos estiverem subterrâneos, proteger de cortes acidentais (por exemplo, com conduítes blindados ou sinalização de presença);

b) segregar cabos de energia de cabos de comunicação para evitar interferências;

c) para sistemas sensíveis ou críticos, outros controles a serem considerados incluem:

   1) instalação de conduítes blindados e salas trancadas ou caixas e alarmes em pontos de inspeção e terminação;

   2) uso de blindagem eletromagnética para proteger os cabos;

   3) varreduras técnicas periódicas e inspeções físicas para detectar dispositivos não autorizados sendo anexados aos cabos;

   4) acesso controlado aos quadros de distribuição e salas de cabeamento (por exemplo, com chaves mecânicas ou PIN);

   5) uso de cabos de fibra óptica;

d) rotular os cabos em cada extremidade com detalhes suficientes de origem e destino, para permitir a identificação física e inspeção do cabo.

Convém procurar orientação especializada sobre como gerenciar riscos decorrentes de incidentes ou mau funcionamento do cabeamento.

Outras informações

Às vezes, cabeamento de energia e telecomunicações são recursos compartilhados para mais de uma organização ocupando instalações compartilhadas.

7.13 Manutenção de equipamentos

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Segurança_física #Gestão_de_ativos	#Proteção #Resiliência

Controle

Convém que os equipamentos sejam mantidos corretamente para assegurar a disponibilidade, integridade e confidencialidade da informação.

Propósito

Evitar perdas, danos, roubos ou comprometimento de informações e outros ativos associados e interrupção das operações da organização causada pela falta de manutenção.

Orientação

Convém que sejam consideradas as seguintes diretrizes para a manutenção dos equipamentos:

a) manutenção de equipamentos de acordo com a frequência e as especificações de serviço recomendadas pelo fornecedor;

b) implantação e monitoramento de um programa de manutenção da organização;

c) apenas pessoal de manutenção autorizado a realizar reparos e manutenção em equipamentos;

d) manutenção de registros de todas as falhas suspeitas ou reais, e de toda a manutenção preventiva e corretiva;

e) implementação de controles adequados quando o equipamento for programado para manutenção, levando em conta se essa manutenção é realizada por pessoal no local ou externamente à organização; condicionando o pessoal de manutenção a um acordo de confidencialidade adequado;

f) fiscalização do pessoal de manutenção durante a realização da manutenção no local;

g) autorização e controle do acesso para manutenção remota;

h) aplicação de medidas de segurança para ativos fora das instalações da organização (ver 7.9), se os equipamentos contendo informações forem retirados das dependências da organização para manutenção;

i) cumprimento de todos os requisitos de manutenção impostos pelo seguro;

j) inspeção do equipamento antes de colocá-lo de volta em operação após a manutenção, para assegurar que o equipamento não tenha sido adulterado e que esteja funcionando corretamente;

k) aplicação de medidas para descarte seguro ou reutilização de equipamentos (ver 7.14), se for determinado que é necessário descartar o equipamento.

Outras informações

O equipamento inclui componentes técnicos de instalações de processamento de informações, UPS e baterias, geradores de energia, alternadores de energia e conversores, sistemas e alarmes de detecção de intrusões físicas, detectores de fumaça, extintores de incêndio, ar-condicionado e elevadores.

7.14 Descarte seguro ou reutilização de equipamentos

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade	#Proteger	#Segurança_física #Gestão_de_ativos	#Proteção

Controle

Convém que sejam verificados os itens dos equipamentos que contenham mídia de armazenamento, para assegurar que quaisquer dados confidenciais e *software* licenciado tenham sido removidos ou substituídos com segurança antes do descarte ou reutilização.

Propósito

Evitar o vazamento de informações por equipamento que seja descartado ou reutilizado.

Orientação

Convém que os equipamentos sejam verificados para garantir se as mídias de armazenamento estão ou não presentes antes do descarte ou reutilização.

Convém que as mídias de armazenamento que contenham informações confidenciais ou com direitos autorais sejam fisicamente destruídas ou que as informações sejam destruídas, excluídas ou sobregravadas usando técnicas para tornar as informações originais não recuperáveis, em vez de se usar a função de exclusão-padrão. Ver 7.10 para obter orientação detalhada sobre o descarte seguro de mídia de armazenamento e 8.10 para orientação sobre a exclusão de informações.

Convém que os rótulos e as marcas que identifiquem a organização ou indiquem a classificação, o proprietário, o sistema ou a rede sejam removidos antes do descarte, incluindo revenda ou doação para caridade.

Convém que a organização considere a remoção de controles de segurança, como controles de acesso ou equipamentos de vigilância, ao fim do contrato de locação ou ao sair do controle da organização. Isso depende de fatores como:

a) o contrato de locação prevê devolver o equipamento na condição original;

b) minimização do risco de deixar sistemas com informações confidenciais no equipamento para o próximo locatário (por exemplo, listas de acesso ao usuário, arquivos de vídeo ou imagem);

c) capacidade de reutilizar os controles na próxima instalação.

Outras informações

Equipamentos danificados que contenham mídia de armazenamento podem requerer um processo de avaliação de risco para determinar se convém que os itens sejam fisicamente destruídos ao invés de enviados para reparo ou descarte. As informações podem ser comprometidas por meio de descarte descuidado ou reutilização de equipamentos.

Adicionalmente à exclusão segura do disco, a criptografia completa do disco reduz o risco de divulgação de informações confidenciais quando o equipamento é descartado ou reutilizado, desde que:

a) o processo de criptografia seja suficientemente forte e abranja todo o disco (incluindo espaço livre, arquivos de paginação);

b) as chaves criptográficas sejam longas o suficiente para resistir a ataques de força bruta;

c) as chaves criptográficas sejam mantidas em sigilo (por exemplo, nunca armazenadas no mesmo disco).

Para obter mais orientações sobre criptografia, ver 8.24.

As técnicas para sobrepor com segurança as mídias de armazenamento diferem de acordo com a tecnologia de mídia de armazenamento e o nível de classificação das informações na mídia de armazenamento. Convém que as ferramentas de sobreposição sejam analisadas criticamente para assegurar que elas sejam aplicáveis à tecnologia da mídia de armazenamento.

Ver a ISO/IEC 27040 para obter detalhes sobre métodos para higienizar a mídia de armazenamento.

8 Controles tecnológicos

8.1 Dispositivos *endpoint* do usuário

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Proteção_da_ informação #Gestão_ de_ativos	#Proteção

Controle

Convém que as informações armazenadas, tratadas ou acessíveis por meio de dispositivos *endpoint* do usuário sejam protegidas.

Propósito

Proteger informações contra os riscos introduzidos pelo uso de dispositivos *endpoint* do usuário.

Orientação

Geral

Convém que a organização estabeleça uma política específica por tema sobre configuração segura e manuseio de dispositivos *endpoint* do usuário. Convém que a política específica por tema seja comunicada a todo o pessoal relevante e que considere o seguinte:

a) tipo de informação e nível de classificação que os dispositivos *endpoint* do usuário podem manusear, tratar, armazenar ou apoiar;

b) registro de dispositivos *endpoint* do usuário;

c) requisitos para proteção física;

d) restrição da instalação de *software* (por exemplo, controlado remotamente por administradores de sistemas);

e) requisitos para o *software* do dispositivo *endpoint* do usuário (incluindo versões de *software*) e para a aplicação de atualizações (por exemplo, atualização automática ativa);

f) regras de conexão com serviços de informação, redes públicas ou qualquer outra rede fora das instalações (por exemplo, exigindo o uso de *firewall* pessoal);

g) controles de acesso;

h) criptografia do dispositivo de armazenamento

i) proteção contra *malware*;

j) desativação, exclusão ou bloqueio remotos;

k) *backup*;

l) uso de serviços *web* e aplicações *web*;

m) análise de comportamento do usuário (ver 8.16);

n) uso de dispositivos removíveis, incluindo dispositivos de memória removíveis, e a possibilidade de desativação de portas físicas (por exemplo, portas USB);

o) uso de capacidade de particionamento, se apoiado pelo dispositivo *endpoint* do usuário, que pode separar com segurança as informações da organização e outros ativos associados (por exemplo, *software*) de outras informações e outros ativos associados no dispositivo.

Convém considerar se certas informações são tão sensíveis que só podem ser acessadas por meio de dispositivos *endpoint* do usuário, mas não ser armazenadas em tais dispositivos. Nesses casos, técnicas adicionais de proteção podem ser necessárias no dispositivo. Por exemplo, assegurar que o *download* de arquivos para trabalho *off-line* seja desativado e que o armazenamento local, como cartão SD, seja desativado.

Na medida do possível, convém que as recomendações sobre este controle sejam aplicadas pela gestão de configuração (ver 8.9) ou por ferramentas automatizadas.

Responsabilidade do usuário

Convém que todos os usuários estejam cientes dos requisitos e procedimentos de segurança para proteger os dispositivos *endpoint* do usuário, bem como de suas responsabilidades para implementar tais medidas de segurança. Convém aconselhar os usuários a:

a) encerrar sessões ativas e finalizar serviços quando não forem mais necessários;

b) proteger dispositivos *endpoint* do usuário contra uso não autorizado com um controle físico (por exemplo, bloqueio de teclas ou fechaduras especiais) e controle lógico (por exemplo, acesso à senha), quando não estiverem em uso; não deixar dispositivos portadores de informações importantes, sensíveis ou críticas de negócios sem supervisão;

c) utilizar dispositivos com cuidados especiais em locais públicos, escritórios abertos, locais de encontro e outras áreas desprotegidas (por exemplo, evitar ler informações confidenciais se as pessoas podem ler por trás, usar filtros de tela de privacidade);

d) proteger fisicamente dispositivos *endpoint* do usuário contra roubo (por exemplo, em carros e outras formas de transporte, quartos de hotel, centros de conferência e locais de reuniões).

Convém estabelecer um procedimento específico que leve em conta requisitos legais, estatutários, regulamentares, contratuais (incluindo seguro) e outros requisitos de segurança da organização para casos de roubo ou perda de dispositivos *endpoint* do usuário.

Uso de dispositivos pessoais

Quando a organização permite o uso de dispositivos pessoais (às vezes conhecidos como BYOD), além da orientação dada neste controle, convém que seja considerado o seguinte:

a) separação do uso pessoal e empresarial dos dispositivos, incluindo o uso de *software* para apoiar tais separação e proteção de dados de negócios em um dispositivo privado;

b) fornecimento de acesso às informações de negócios somente após os usuários terem reconhecido suas funções (proteção física, atualização de *software* etc.), dispensando a propriedade de dados do negócio, permitindo a limpeza remota de dados pela organização em caso de roubo ou perda do dispositivo ou quando não estiver mais autorizado a usar o serviço. Nesses casos, convém considerar a legislação de proteção de DP;

c) políticas e procedimentos específicos por tema para evitar disputas relativas a direitos de propriedade intelectual desenvolvidos em equipamentos de propriedade privada.

d) acesso a equipamentos de propriedade privada (para verificar a segurança da máquina ou durante uma investigação) que pode ser impedido pela legislação;

e) contratos de licenciamento de *software* que permitem que as organizações sejam responsáveis pelo licenciamento de *software* do cliente em dispositivos *endpoint* de usuário, de propriedade privada de funcionários ou de usuários externos.

Conexões sem fio

Convém que a organização estabeleça procedimentos para:

a) a configuração de conexões sem fio em dispositivos (por exemplo, desativação de protocolos vulneráveis);

b) uso de conexões sem fio ou com fio com largura de banda apropriada, de acordo com as políticas específicas por tema (por exemplo, porque cópias de segurança ou atualizações de *software* são necessárias).

Outras informações

Os controles para proteger informações em dispositivos *endpoint* do usuário dependem se o dispositivo *endpoint* do usuário é usado apenas dentro das instalações seguras e conexões de rede da organização, ou se ele está exposto a ameaças físicas e relacionadas à rede aumentadas fora da organização.

As conexões sem fio para dispositivos *endpoint* do usuário são semelhantes a outros tipos de conexões de rede, mas têm diferenças importantes que convém que sejam consideradas ao identificar controles. Em particular, o *backup* das informações armazenadas em dispositivos *endpoint* do usuário às vezes pode falhar, devido à largura de banda de rede limitada ou porque os dispositivos *endpoint* do usuário não estão conectados nos momentos em que os *backups* são agendados.

Para algumas portas USB, como USB-C, desativar a porta USB não é possível porque ela é usada para outros propósitos (por exemplo, fornecimento de energia e saída de monitor).

8.2 Direitos de acessos privilegiados

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Gestão_de_ identidade_e_acesso	#Proteção

Controle

Convém restringir e gerenciar a atribuição e o uso de direitos de acessos privilegiados.

Propósito

Assegurar que apenas usuários, componentes de *software* e serviços autorizados recebam direitos de acessos privilegiados.

Orientação

Convém que a atribuição de direitos de acesso privilegiado seja controlada por meio de um processo de autorização de acordo com a política específica por tema de controle de acessos (ver 5.15). Convém considerar:

a) identificar usuários que precisem de direitos de acesso privilegiados para cada sistema ou processo (por exemplo, sistemas operacionais, sistemas de gerenciamento de banco de dados e aplicações);

b) atribuir direitos de acesso privilegiado aos usuários conforme necessário e em um princípio de evento por evento, em consonância com a política específica por tema de controle de acesso (ver 5.15) (ou seja, apenas para indivíduos com a competência necessária para realizar atividades que exijam acesso privilegiado e com base no requisito mínimo para seus papéis funcionais);

c) manter um processo de autorização (ou seja, determinar quem pode aprovar direitos de acesso privilegiado, ou não conceder direitos de acesso privilegiado até que o processo de autorização seja concluído) e um registro de todos os privilégios alocados;

d) definir e implementar requisitos para o término dos direitos de acesso privilegiado;

e) tomar medidas para assegurar que os usuários estejam cientes de seus direitos de acesso privilegiados e quando estão no modo de acesso privilegiado. As medidas possíveis incluem o uso de identidades específicas do usuário, configurações de interface do usuário ou até mesmo equipamentos específicos;

f) os requisitos de autenticação para direitos de acesso privilegiados podem ser maiores do que os requisitos para os direitos normais de acesso. Reautenticação ou reforço na autenticação podem ser necessários antes de fazer o trabalho com direitos de acesso privilegiados;

g) regularmente, e após qualquer mudança organizacional, analisar criticamente os usuários trabalhando com direitos de acesso privilegiados, a fim de verificar se suas funções, papéis, responsabilidades e competências ainda os qualificam para trabalhar com direitos de acesso privilegiados (ver 5.18);

h) estabelecer regras específicas para evitar o uso de ID genéricos de usuário de administração (como “root”), dependendo dos recursos de configuração dos sistemas. Gerenciar e proteger informações de autenticação destas identidades (ver 5.17);

i) conceder acesso privilegiado temporário apenas pelo período necessário para implementar alterações ou atividades aprovadas (por exemplo, para atividades de manutenção ou algumas mudanças críticas), em vez de conceder permanentemente direitos de acesso privilegiado. Isso é frequentemente referido como procedimento de “quebre o vidro” e, muitas vezes, automatizado por tecnologias de gerenciamento de acesso privilegiado;

j) registrar todo o acesso privilegiado ao sistema para fins de auditoria;

k) não compartilhar ou vincular identidades com direitos de acesso privilegiados a várias pessoas, atribuindo a cada pessoa uma identidade separada que permita atribuir direitos específicos de acesso privilegiado. As identidades podem ser agrupadas (por exemplo, definindo um grupo administrador), a fim de simplificar a gestão dos direitos de acesso privilegiados;

l) usar identidades com direitos de acesso privilegiados apenas para a realização de tarefas administrativas e não para tarefas gerais do dia a dia [ou seja, verificar e-mails, acessar a *web* (convém que os usuários tenham uma identidade de rede normal separada para essas atividades)].

Outras informações

Direitos de acesso privilegiados são direitos de acesso fornecidos a uma identidade, um papel ou um processo, que permitem a realização de atividades que usuários ou processos típicos não estão aptos a realizar. Os papéis de administrador do sistema normalmente exigem direitos de acesso privilegiados.

O uso inadequado de privilégios de administrador do sistema (qualquer recurso ou facilidade de um sistema de informações que permita ao usuário sobrepor controles de sistema ou aplicações) é um dos principais fatores contribuintes para falhas ou violações de sistemas.

Mais informações relacionadas à gestão de acesso e à gestão segura dos recursos de tecnologias de informação e informação e comunicação podem ser encontradas na ISO/IEC 29146.

8.3 Restrição de acesso à informação

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Gestão_de_ identidade_e_acesso	#Proteção

Controle

Convém que o acesso às informações e outros ativos associados seja restrito de acordo com a política específica por tema sobre controle de acesso.

Propósito

Assegurar apenas o acesso autorizado e impedir o acesso não autorizado a informações e a outros ativos associados.

Orientação

Convém restringir o acesso a informações e a outros ativos associados, de acordo com as políticas específicas por tema. Para apoiar os requisitos de restrição de acesso, convém considerar:

a) não permitir acesso a informações confidenciais por identidades de usuários desconhecidos ou anonimamente. Convém que o acesso público ou anônimo só seja concedido a locais de armazenamento que não contenham informações confidenciais;

b) fornecer mecanismos de configuração para controlar o acesso à informação em sistemas, aplicações e serviços;

c) controlar quais dados podem ser acessados por um determinado usuário;

d) controlar quais identidades ou grupo de identidades têm acesso, como ler, escrever, excluir e executar;

e) fornecer controles de acesso físico ou lógico para o isolamento de aplicações sensíveis, dados de aplicações sensíveis ou sistemas sensíveis.

Além disso, convém considerar técnicas e processos dinâmicos de gestão de acesso para proteger informações confidenciais que tenham alto valor para a organização, quando:

a) precisar de controle granular sobre quem pode acessar tais informações, durante qual o período e de que forma;

b) quiser compartilhar tais informações com pessoas fora da organização e manter o controle sobre quem pode acessá-lo;

c) quiser gerenciar dinamicamente, em tempo real, o uso e a distribuição dessas informações;

d) quiser proteger essas informações contra alterações não autorizadas, cópia e distribuição (incluindo impressão);

e) quiser monitorar o uso das informações;

f) quiser registrar quaisquer alterações que ocorram nessas informações, para o caso de uma futura investigação, se necessária.

Convém que as técnicas dinâmicas de gestão de acesso protejam as informações durante todo o seu ciclo de vida (ou seja, criação, tratamento, armazenamento, transmissão e descarte), incluindo:

a) estabelecer regras sobre a gestão de acesso dinâmico com base em casos específicos de uso, considerando:

   1) conceder permissões de acesso com base em identidade, dispositivo, localização ou aplicação;

   2) aproveitar o esquema de classificação para determinar quais informações precisam ser protegidas com técnicas dinâmicas de gerenciamento de acesso;

b) estabelecer processos operacionais, de monitoramento e de comunicação, e suporte à infraestrutura técnica.

Convém que os sistemas dinâmicos de gestão de acesso protejam as informações por meio de:

a) exigência de autenticação, credenciais apropriadas ou um certificado para acessar informações;

b) restrição do acesso, por exemplo, por um prazo especificado (por exemplo, após uma determinada data ou até uma data específica);

c) uso de criptografia para proteger informações;

d) determinação de permissões de impressão das informações;

e) registro de quem acessa as informações e como as informações são usadas;

f) disparo de alertas, se tentativas de usar indevidamente as informações forem detectadas.

Outras informações

Técnicas dinâmicas de gestão de acesso e outras tecnologias dinâmicas de proteção da informação podem apoiar a proteção das informações mesmo quando os dados são compartilhados além da organização originária, onde os controles de acesso tradicionais não podem ser aplicados. Elas podem ser aplicadas a documentos, *e-mails* ou outros arquivos contendo informações, para limitar quem pode acessar o conteúdo e de que forma. Elas podem ser em um nível granular e ser adaptadas ao longo do ciclo de vida das informações.

As técnicas dinâmicas de gestão de acesso não substituem a gestão clássica de acesso [por exemplo, usando listas de controle de acesso (ACL)], mas podem adicionar mais fatores para condicionalidade, avaliação em tempo real, redução de dados *just-in-time* e outros aprimoramentos que podem ser úteis para as informações mais sensíveis. Elas oferecem uma maneira de controlar o acesso fora do ambiente da organização. A resposta a incidentes pode ser apoiada por técnicas dinâmicas de gestão de acesso, pois as permissões podem ser modificadas ou revogadas a qualquer momento.

Informações adicionais sobre uma estrutura para gestão de acesso são fornecidas na ISO/IEC 29146.

8.4 Acesso ao código-fonte

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Gestão_de_identidade_e_acesso #Segurança_de_aplicação #Segurança_de_configuração	#Proteção

Controle

Convém que os acessos de leitura e escrita ao código-fonte, ferramentas de desenvolvimento e bibliotecas de *software* sejam adequadamente gerenciados.

Propósito

Evitar a introdução de funcionalidades não autorizadas, prevenir mudanças não intencionais ou maliciosas e manter a confidencialidade de propriedade intelectual valiosa.

Orientação

Convém que o acesso ao código-fonte e aos itens associados (como projetos, especificações, planos de verificação e planos de validação) e ferramentas de desenvolvimento (por exemplo, compiladores, construtores, ferramentas de integração, plataformas de teste e ambientes) seja estritamente controlado.

Para o código-fonte, isso pode ser alcançado controlando o armazenamento central de tal código, de preferência no sistema de gerenciamento de código-fonte.

Acesso de leitura e acesso de escrita ao código-fonte podem diferir com base no papel do pessoal. Por exemplo, o acesso de leitura ao código-fonte pode ser amplamente fornecido dentro da organização, mas o acesso à gravação ao código-fonte só é disponibilizado para pessoas privilegiadas ou proprietários designados. Quando os componentes de código são usados por vários desenvolvedores dentro de uma organização, convém que um acesso de leitura a um repositório centralizado de código seja implementado. Além disso, se o código-fonte aberto ou componentes de código de terceiros forem usados dentro de uma organização, o acesso de leitura a esses repositórios de código externo pode ser amplamente fornecido. No entanto, convém que o acesso de gravação ainda seja restrito.

Convém que as seguintes diretrizes sejam consideradas para controlar o acesso às bibliotecas de código do programa, a fim de reduzir o potencial de corrupção de programas de computador:

a) gerenciar o acesso ao código-fonte do programa e às bibliotecas de origem do programa de acordo com procedimentos estabelecidos;

b) conceder acesso de leitura e de escrita ao código-fonte com base nos requisitos de negócio e na gestão de tratativas de riscos de alteração ou uso indevido e de acordo com procedimentos estabelecidos;

c) atualizar o código-fonte e os itens associados, conceder acesso ao código-fonte de acordo com os procedimentos de controle de mudança (ver 8.32) e somente executá-lo após a autorização adequada ter sido recebida;

d) não conceder aos desenvolvedores acesso direto ao repositório de código-fonte, mas sim por meio de ferramentas de desenvolvedor que controlem atividades e autorizações no código-fonte;

e) armazenar listagem dos programas em um ambiente seguro, onde o acesso à leitura e escrita seja devidamente gerenciado e atribuído;

f) manter um registro de auditoria de todos os acessos e de todas as alterações no código-fonte.

Se o código-fonte do programa for destinado a ser publicado, convém que sejam considerados controles adicionais para fornecer garantia sobre a sua integridade (por exemplo, assinatura digital).

Outras informações

Se o acesso ao código-fonte não for devidamente controlado, o código-fonte pode ser modificado ou alguns dados no ambiente de desenvolvimento (por exemplo, cópias de dados de produção, detalhes de configuração) podem ser recuperados por pessoas não autorizadas.

8.5 Autenticação segura

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Gestão_de_ identidade_e_ acesso	#Proteção

Controle

Convém que sejam implementadas tecnologias e procedimentos de autenticação seguros, com base em restrições de acesso à informação e à política específica por tema de controle de acesso.

Propósito

Assegurar que um usuário ou uma entidade seja autenticada com segurança, quando o acesso a sistemas, aplicações e serviços é concedido.

Orientação

Convém que seja escolhida uma técnica de autenticação adequada para comprovar a identidade alegada de um usuário, *software*, mensagens e outras entidades.

Convém que a força da autenticação seja adequada para a classificação das informações a serem acessadas. Quando for necessária uma autenticação forte e verificação de identidade, convém usar métodos de autenticação alternativos a senhas, como certificados digitais, cartões inteligentes, *tokens* ou meios biométricos.

Convém que as informações de autenticação sejam acompanhadas de fatores adicionais de autenticação para acessar sistemas de informação críticos (também conhecidos como autenticação multifatores). Usar uma combinação de múltiplos fatores de autenticação, como o que você sabe, o que você tem e o que você é, reduz as possibilidades de acessos não autorizados. A autenticação multifatores pode ser combinada com outras técnicas para exigir fatores adicionais em circunstâncias específicas, com base em regras e padrões predefinidos, como o acesso a partir de um local incomum, a partir de um dispositivo incomum ou em um momento incomum.

Convém que as informações de autenticação biométrica sejam invalidadas se alguma vez forem comprometidas. A autenticação biométrica pode estar indisponível, dependendo das condições de uso (por exemplo, umidade ou envelhecimento). Para se preparar para essas questões, convém que a autenticação biométrica seja acompanhada de pelo menos uma técnica alternativa de autenticação.

Convém que o procedimento para entrada em um sistema ou aplicativo seja projetado para minimizar o risco de acesso não autorizado. Convém que os procedimentos e tecnologias de acesso ao sistema sejam implementados considerando o seguinte:

a) não exibir informações sensíveis do sistema ou do aplicativo até que o processo de *log-on* no sistema tenha sido concluído com sucesso, a fim de evitar fornecer a um usuário não autorizado qualquer assistência desnecessária;

b) exibir um aviso público de que convém que o sistema, aplicativo ou serviço só sejam acessados por usuários autorizados;

c) não fornecer mensagens de ajuda durante o procedimento de acesso ao sistema que auxiliariam um usuário não autorizado (por exemplo, se houver uma condição de erro, não convém que o sistema indique qual parte dos dados está correta ou incorreta);

d) validar as informações de *log-on* no sistema somente na conclusão de todos os dados de entrada;

e) proteger contra tentativas de *log-on* com força bruta em nomes de usuário e senhas (por exemplo, usando o CAPTCHA, exigindo redefinição de senha após um número predefinido de tentativas fracassadas ou bloqueando o usuário após um número máximo de erros);

f) registrar as tentativas malsucedidas e bem-sucedidas;

g) criar um evento de segurança, se for detectada uma possível tentativa ou violação bem-sucedida de controles de acesso ao sistema (por exemplo, enviando um alerta para o usuário e os administradores do sistema da organização quando um determinado número de tentativas erradas de senha foi alcançado);

h) exibir ou enviar as seguintes informações em um canal separado na conclusão de um acesso bem-sucedido:

   1) data e hora do *log-on* anterior bem-sucedido ao sistema;

   2) detalhes de quaisquer tentativas de *log-on* malsucedidas desde o último *log-on* bem-sucedido ao sistema;

i) não exibir a senha em texto claro quando ela estiver sendo inserida; em alguns casos, pode ser necessário desativar essa funcionalidade para facilitar o acesso ao sistema pelo usuário (por exemplo, por razões de acessibilidade ou para evitar o bloqueio de usuários por causa de erros repetidos);

j) não transmitir senhas em texto claro pela rede para evitar a captura por um programa de “sniffer” de rede;

k) finalizar sessões inativas após um período especificado de inatividade, especialmente em locais de alto risco, como áreas públicas ou externas fora da gestão de segurança da organização ou em dispositivos de terminal do usuário;

l) restringir os tempos de duração da conexão para fornecer segurança adicional para aplicações de alto risco e reduzir a janela de oportunidade para acesso não autorizado.

Outras informações

Informações adicionais sobre a garantia de autenticação de entidade podem ser encontradas na ISO/IEC 29115.

8.6 Gestão de capacidade

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo #Detectivo	#Integridade #Disponibilidade	#Identificar #Detectar #Proteger	#Continuidade	#Governança_e_ecossistema #Proteção

Controle

Convém que o uso dos recursos seja monitorado e ajustado de acordo com os requisitos atuais e esperados de capacidade.

Propósito

Assegurar a capacidade necessária dos recursos de tratamento de informações, recursos humanos, escritórios e outros serviços de infraestrutura.

Orientação

Convém que sejam identificados os requisitos de capacidade para recursos de tratamento de informações, recursos humanos, escritórios e outros serviços de infraestrutura, levando em conta a criticidade dos negócios dos sistemas e processos em questão.

Convém que sejam aplicados ajuste e monitoramento do sistema para assegurar e, se necessário, melhorar a disponibilidade e a eficiência dos sistemas.

Convém que a organização realize testes de estresse de sistemas e serviços para confirmar que a capacidade suficiente do sistema está disponível para atender aos requisitos de desempenho máximo.

Convém que os controles detectivos sejam colocados em prática para indicar problemas no devido tempo.

Para projeções dos requisitos futuros de capacidade, convém levar em conta os novos requisitos de negócios e sistemas, tendências atuais e projetadas nos recursos de tratamento de informações da organização.

Convém dar atenção especial a quaisquer recursos com prazos de aquisição longos ou custos elevados. Portanto, convém que os gestores, proprietários de serviços ou produtos monitorem a utilização dos principais recursos do sistema.

Convém que os gestores usem informações de capacidade para identificar e evitar possíveis limitações de recursos e dependência de pessoas-chave que possam apresentar uma ameaça à segurança do sistema ou serviços e planejar ações apropriadas.

A capacidade suficiente pode ser alcançada aumentando a capacidade ou reduzindo a demanda.

Convém que o seguinte seja considerado para aumentar a capacidade:

a) contratação de pessoal novo;

b) obtenção de novas instalações ou espaço;

c) aquisição de sistemas de tratamento mais potentes, memória e armazenamento;

d) uso da computação em nuvem, que possui características inerentes que abordam diretamente as questões de capacidade. A computação em nuvem tem elasticidade e escalabilidade que permitem a rápida expansão sob demanda e a redução dos recursos disponíveis para aplicações e serviços específicos.

Convém que seja considerado o seguinte, para reduzir a demanda sobre os recursos da organização:

a) excluir dados obsoletos (espaço em disco);

b) descartar registros impressos que tenham cumprido seu período de retenção (liberar espaço para prateleiras);

c) descomissionar aplicações, sistemas, bancos de dados ou ambientes;

d) otimizar processos em lote e agendamentos;

e) otimizar código de aplicativo ou consultas de banco de dados;

f) negar ou restringir a largura de banda para serviços com consumo de recursos, se estes não forem críticos (por exemplo, *streaming* de vídeo).

Para sistemas de missão crítica, convém que seja considerado um plano de gestão de capacidade documentado.

Outras informações

Para obter mais detalhes sobre a elasticidade e escalabilidade da computação em nuvem, ver a ISO/IEC TS 23167.

8.7 Proteção contra *malware*

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo #Detectivo #Corretivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger #Detectar	#Segurança_de_sistemas_e_rede #Proteção_da_ informação	#Proteção #Defesa

Controle

Convém que a proteção contra *malware* seja implementada e apoiada pela conscientização adequada do usuário.

Propósito

Assegurar que informações e outros ativos associados estejam protegidos contra *malware*.

Orientação

Convém que a proteção contra *malware* seja baseada em *software* de detecção e reparo de *malware*, conscientização sobre segurança da informação, acesso adequado aos sistemas e controles de gestão de mudanças. O uso de *software* de detecção e reparo de *malware* sozinho não costuma ser adequado. Convém considerar as seguinte orientações:

a) implementar regras e controles que impeçam ou detectem o uso de *software* não autorizado [por exemplo, lista de aplicações permitidos (ou seja, uso de uma lista que fornece aplicações autorizadas)] (ver 8.19 e 8.32);

b) implementar controles que previnam ou detectem o uso de *sites* maliciosos conhecidos ou suspeitos (por exemplo, lista de bloqueio);

c) reduzir vulnerabilidades que possam ser exploradas por *malware* [por exemplo, por meio de gestão de vulnerabilidades técnicas (ver 8.8 e 8.19)];

d) realizar validação automatizada regular do *software* e do conteúdo de dados dos sistemas, especialmente para sistemas que suportem processos de negócios críticos; investigar a presença de quaisquer arquivos não aprovados ou alterações não autorizadas;

e) estabelecer medidas de proteção contra riscos associados à obtenção de arquivos e *softwares* de redes externas ou em qualquer outro meio;

f) instalar e atualizar regularmente o *software* de detecção *malware* e recorrer ao *software* para varrer computadores e mídia de armazenamento eletrônico. Realizar varreduras regulares inclui:

   1) varrer quaisquer dados recebidos por meio de redes ou de qualquer forma de mídia de armazenamento eletrônico para identificar *malware* antes do uso;

   2) varrer anexos de *e-mail*, mensagens instantâneas e *downloads* em busca de *malware* antes do uso. Realizar essa varredura em diferentes locais (por exemplo, em servidores de *e-mail*, computadores *desktop*) e ao entrar na rede da organização;

   3) varrer páginas da *web* em busca de *malware,* quando acessadas;

g) determinar a atribuição e configuração de ferramentas de detecção e reparo de *malware* com base nos resultados da avaliação de risco e considerando:

   1) princípios de defesa em profundidade onde possam ser mais efetivos. Por exemplo, isso pode levar à detecção de *malware* em um *gateway* de rede (em vários protocolos de aplicações, como *e-mail*, transferência de arquivos e *web*), bem como dispositivos *endpoint* do usuário e servidores;

   2) as técnicas evasivas dos atacantes (por exemplo, o uso de arquivos criptografados) para fornecer *malware* ou o uso de protocolos de criptografia para transmitir *malware*;

h) ter cuidado para proteger contra a introdução de *malware* durante os procedimentos de manutenção e emergência, que podem contornar controles normais contra *malware*;

i) implementar um processo para autorizar desativar temporariamente ou permanentemente algumas ou todas as medidas contra *malware*, incluindo autoridades de aprovação de exceção, justificativa documentada e data da análise crítica. Isso pode ser necessário quando a proteção contra *malware* causar disrupção em operações normais;

j) elaborar planos adequados de continuidade de negócios para recuperação de ataques de *malware*, incluindo todas as cópias de segurança de dados e *software* necessários (incluindo cópia de segurança *on-line* e *off-line)* e medidas de recuperação (ver 8.13);

k) isolar ambientes onde consequências catastróficas possam ocorrer;

l) determinar procedimentos e responsabilidades para lidar com a proteção contra *malware* em sistemas, incluindo treinamento em seu uso, emissão de comunicação e recuperação de ataques de *malware*;

m) prover conscientização ou treinamento (ver 6.3) a todos os usuários sobre como identificar e potencialmente mitigar o recebimento, envio ou instalação de *e-mails*, arquivos ou programas infectados por *malware* [as informações coletadas em n) e em o) podem ser usadas para assegurar que a conscientização e o treinamento sejam mantidos atualizados];

n) implementar procedimentos para coletar regularmente informações sobre novos *malwares*, por exemplo, assinar listas de discussão ou analisar criticamente *websites* relevantes;

o) verificar se informações relacionadas a *malware*, como as de boletins de aviso, vêm de fontes qualificadas e respeitáveis (por exemplo, *sites* confiáveis da *internet* ou fornecedores de *software* de detecção de *malware*) e se são precisas e informativas.

Outras informações

Nem sempre é possível instalar *software* que proteja contra *malware* em alguns sistemas (por exemplo, alguns sistemas de controle industrial). Algumas formas de *malware* infectam sistemas operacionais de computador e o *firmware* de computador de tal forma que os controles comuns de *malware* não estão aptos a limpar o sistema por completo, e uma reinstalação completa do *software* do sistema operacional, e às vezes do *firmware* do computador, pode ser necessária para retornar a um estado seguro.

8.8 Gestão de vulnerabilidades técnicas

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Identificar #Proteger	#Gestão_de_ameaças_e_vulnerabilidades	#Proteção #Defesa

Controle

Convém que informações sobre vulnerabilidades técnicas dos sistemas de informação em uso sejam obtidas, a exposição da organização a tais vulnerabilidades sejam avaliadas e medidas apropriadas sejam tomadas.

Propósito

Evitar a exploração de vulnerabilidades técnicas.

Orientação

Identificando vulnerabilidades técnicas

Convém que a organização tenha um inventário preciso de ativos (ver 5.9 a 5.14) como pré-requisito para a gestão eficaz de vulnerabilidade técnica; convém que o inventário inclua o *fornecedor* de *software*, nome do *software*, números de versão, estado atual de implantação (por exemplo, qual software está instalado em quais sistemas) e a(s) pessoa(s) dentro da organização responsável(is) pelo *software*.

Convém que, para identificar vulnerabilidades técnicas, a organização considere:

a) definir e estabelecer os cargos e responsabilidades associados à gestão de vulnerabilidades técnicas, incluindo monitoramento de vulnerabilidades, processo de avaliação de risco de vulnerabilidade, atualização, rastreamento de ativos e quaisquer responsabilidades de coordenação necessárias;

b) para *software* e outras tecnologias (com base na lista de inventário de ativos, ver 5.9), identificar recursos de informações que serão utilizados para identificar vulnerabilidades técnicas relevantes e manter a conscientização sobre elas. Atualizar a lista de recursos de informação com base em alterações no inventário ou quando outros recursos novos ou úteis forem encontrados;

c) exigir fornecedores de sistema de informação (incluindo seus componentes) para garantir relatórios, manuseio e divulgação de vulnerabilidades, incluindo os requisitos nos contratos aplicáveis (ver 5.20);

d) utilizar ferramentas de varredura de vulnerabilidades adequadas às tecnologias em uso para identificar vulnerabilidades e verificar se a correção de vulnerabilidades foi bem-sucedida;

e) realizar testes de invasão planejados, documentados e repetíveis ou avaliações de vulnerabilidade por pessoas competentes e autorizadas para apoiar a identificação de vulnerabilidades. Exercer cautela com tais atividades pode levar a um compromisso da segurança do sistema;

f) rastrear o uso de bibliotecas de terceiros e código-fonte para vulnerabilidades. Convém que isso seja incluído em codificação segura (ver 8.28).

Convém que a organização desenvolva procedimentos e capacidades para:

a) detectar a existência de vulnerabilidades em seus produtos e serviços, incluindo qualquer componente externo utilizado nestes;

b) receber relatórios de vulnerabilidade de fontes internas ou externas.

Convém que a organização forneça um ponto de contato público como parte de uma política específica por tema sobre a vulnerabilidade da divulgação, para que pesquisadores e outros sejam capazes de relatar problemas. Convém que as organizações estabeleçam procedimentos de emissão de relatórios de vulnerabilidade, formulários de emissão de relatórios *on-line* e uso de fóruns apropriados de inteligência de ameaças ou compartilhamento de informações. Convém que as organizações também considerem programas de recompensa por *bugs* em que as recompensas sejam oferecidas como um incentivo para ajudar as organizações na identificação de vulnerabilidades, a fim de corrigi-las adequadamente.

Convém que a organização também compartilhe informações com órgãos competentes do setor ou outras partes interessadas.

Avaliando vulnerabilidades técnicas

Para avaliar as vulnerabilidades técnicas identificadas, convém que a organização considere as seguintes orientações:

a) analisar e verificar relatórios para determinar qual atividade de resposta e remediação é necessária;

b) uma vez identificada uma potencial vulnerabilidade técnica, identificar os riscos associados e as ações a serem tomadas. Tais ações podem envolver a atualização de sistemas vulneráveis ou a aplicação de outros controles.

Tomando as medidas adequadas para enfrentar as vulnerabilidades técnicas

Convém que um processo de gerenciamento de atualização de *software* seja implementado para assegurar que os *patches* aprovados mais atualizados e as atualizações do aplicativo sejam instalados para todos os *softwares* autorizados. Se forem necessárias alterações, convém que o *software* original seja retido e as alterações sejam aplicadas a uma cópia designada. Convém que todas as alterações sejam totalmente testadas e documentadas, para que possam ser reaplicadas, se necessário, a futuras atualizações de *software*. Se necessário, convém que as modificações sejam testadas e validadas por um órgão de avaliação independente.

Convém que as seguintes orientações sejam consideradas para abordar vulnerabilidades técnicas:

a) tomar medidas adequadas e oportunas em resposta à identificação de potenciais vulnerabilidades técnicas; definir um cronograma para reagir às notificações de vulnerabilidades técnicas potencialmente relevantes;

b) dependendo da urgência de uma vulnerabilidade técnica a ser tratada, realizar a ação de acordo com os controles relacionados à gestão de mudanças (ver 8.32) ou seguir os procedimentos de resposta a incidentes de segurança da informação (ver 5.26);

c) apenas usar atualizações de fontes legítimas (que podem ser internas ou externas para a organização);

d) testar e avaliar as atualizações antes de serem instaladas, para assegurar que sejam eficazes e não resultem em efeitos colaterais que não podem ser tolerados [ou seja, se houver uma atualização disponível, avaliar os riscos associados à instalação da atualização (convém que os riscos representados pela vulnerabilidade sejam comparados com o risco de instalação da atualização)];

e) abordar sistemas de alto risco primeiro;

f) desenvolver remediação (normalmente atualizações de *software* ou *patches*);

g) testar para confirmar se a remediação ou mitigação é eficaz;

h) fornecer mecanismos para verificar a autenticidade da remediação;

i) se nenhuma atualização estiver disponível ou a atualização não puder ser instalada, considerar outros controles, como:

   1) aplicar qualquer solução alternativa sugerida pelo fornecedor de *software* ou outras fontes relevantes;

2) desligar serviços ou recursos relacionados à vulnerabilidade;

3) adaptar ou adicionar controles de acesso (por exemplo, *firewalls*) nas bordas da rede (ver 8.20 a 8.22);

4) blindar sistemas, dispositivos ou aplicações vulneráveis contra ataques por meio da implantação de filtros de tráfego adequados (às vezes chamados de *patches* virtuais);

5) aumentar o monitoramento para detectar ataques reais;

6) conscientizar sobre a vulnerabilidade.

Para o *software* adquirido, se os fornecedores liberarem regularmente informações sobre atualizações de segurança para seu *software* e fornecerem uma facilidade para instalar essas atualizações automaticamente, convém que a organização decida se pode usar a atualização automática ou não.

Outras considerações

Convém que um registro de auditoria seja mantido para todas as etapas empreendidas na gestão de vulnerabilidade técnica.

Convém que o processo técnico de gestão de vulnerabilidades seja regularmente monitorado e avaliado para assegurar sua eficácia e eficiência.

Convém que um processo técnico eficaz de gestão de vulnerabilidade esteja alinhado com as atividades de gestão de incidentes, para comunicar dados sobre vulnerabilidades à função de resposta a incidentes e fornecer procedimentos técnicos a serem realizados no caso de um incidente ocorrer.

Quando a organização usa um serviço em nuvem fornecido por um provedor de serviços em nuvem de terceiros, convém que a gestão de vulnerabilidade técnica dos recursos do provedor de serviços em nuvem seja assegurada pelo provedor de serviços em nuvem. Convém que as responsabilidades do provedor de serviços em nuvem para a gestão de vulnerabilidades técnicas façam parte do contrato de serviços em nuvem e que isso inclua os processos para relatar as ações do provedor de serviços em nuvem relacionadas a vulnerabilidades técnicas (ver 5.23). Para alguns serviços em nuvem, existem responsabilidades respectivas para o provedor de serviços em nuvem e para o cliente de serviços em nuvem. Por exemplo, o cliente de serviços em nuvem é responsável pela gestão de vulnerabilidades de seus próprios ativos usados para os serviços em nuvem.

Outras informações

A gestão de vulnerabilidades técnicas pode ser vista como uma subfunção da gestão de mudanças e, como tal, pode aproveitar os processos e procedimentos de gestão de mudanças (ver 8.32).

Existe a possibilidade de uma atualização não resolver o problema adequadamente e ter efeitos colaterais negativos. Além disso, em alguns casos, a desinstalação de uma atualização não pode ser facilmente alcançada, uma vez que a atualização tenha sido aplicada.

Se não for possível o teste adequado das atualizações (por exemplo, por causa de custos ou falta de recursos), pode ser considerado um atraso na atualização para avaliar os riscos associados, com base na experiência relatada por outros usuários. O uso da ISO/IEC 27031 pode ser benéfico.

Quando *patches* de *software* ou atualizações são produzidos, a organização pode considerar fornecer um processo de atualização automatizado em que essas atualizações sejam instaladas em sistemas

ou produtos afetados sem a necessidade de intervenção do cliente ou do usuário. Se um processo de atualização automatizada for oferecido, ele pode permitir que o cliente ou o usuário escolha uma opção para desativar a atualização automática ou controlar o horário da instalação da atualização.

Quando o fornecedor provê um processo de atualização automatizado e as atualizações podem ser instaladas em sistemas ou produtos afetados sem a necessidade de intervenção, a organização determina se aplica o processo automatizado ou não. Uma das razões para não optar por atualização automatizada é manter o controle sobre quando a atualização é realizada. Por exemplo, não é possível atualizar um *software* usado para uma operação de negócios até que a operação seja concluída.

Uma fragilidade na varredura de vulnerabilidade é que existe a possibilidade de que ela não responda totalmente para a defesa em profundidade: duas contramedidas que são sempre aplicadas em sequência podem ter vulnerabilidades que são mutuamente mascaradas por pontos fortes. A contramedida composta não é vulnerável, enquanto uma varredura de vulnerabilidade pode informar que ambos os componentes são vulneráveis. Convém que as organizações, portanto, tenham cuidado na análise crítica e atuação em relatórios de vulnerabilidade.

Muitas organizações fornecem *softwares*, sistemas, produtos e serviços não apenas dentro da organização, mas também para as partes interessadas, como clientes, parceiros ou outros usuários. Esses *softwares*, sistemas, produtos e serviços podem ter vulnerabilidades de segurança da informação que afetam a segurança dos usuários.

As organizações podem liberar a remediação e divulgar informações sobre vulnerabilidades aos usuários (normalmente por meio de uma assessoria pública) e fornecer informações apropriadas para serviços de banco de dados de vulnerabilidade de *software*.

Para obter mais informações relacionadas à gestão de vulnerabilidades técnicas ao usar a computação em nuvem, ver a série ISO/IEC 19086 e a ABNT NBR ISO/IEC 27017.

A ISO/IEC 29147 fornece informações detalhadas sobre o recebimento de relatórios de vulnerabilidade e a publicação de avisos de vulnerabilidade. A ISO/IEC 30111 fornece informações detalhadas sobre o manuseio e a resolução de vulnerabilidades relatadas.

8.9 Gestão de configuração

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Configuração_segura	#Proteção

Controle

Convém que as configurações, incluindo configurações de segurança, de *hardware*, *software*, serviços e redes sejam estabelecidas, documentadas, implementadas, monitoradas e analisadas criticamente.

Propósito

Assegurar que o *hardware*, o *software*, os serviços e as redes funcionem corretamente com as configurações de segurança necessárias, e que a configuração não seja alterada por alterações não autorizadas ou incorretas.

Orientação

Geral

Convém que a organização defina e implemente processos e ferramentas para impor as configurações definidas (incluindo configurações de segurança) para *hardware*, *software*, serviços (por exemplo, serviços em nuvem) e redes, para sistemas recém-instalados, bem como para sistemas operacionais ao longo de sua vida útil.

Convém que papéis, responsabilidades e procedimentos estejam em vigor para assegurar o controle satisfatório de todas as alterações de configuração.

Modelos-padrão

Convém que os modelos-padrão para a configuração segura de *hardware*, *software*, serviços e redes sejam definidos:

a) usando orientação disponível publicamente (por exemplo, modelos predefinidos de fornecedores e de organizações de segurança independentes);

b) considerando o nível de proteção necessário para determinar um nível suficiente de segurança;

c) apoiando a política de segurança da informação da organização, políticas específicas por tema, normas e outros requisitos de segurança;

d) considerando a viabilidade e aplicabilidade das configurações de segurança no contexto da organização.

Convém que os modelos sejam analisados criticamente de forma periódica e atualizados quando novas ameaças ou vulnerabilidades precisarem ser abordadas, ou quando novas versões de *software* ou *hardware* forem introduzidas.

Convém que sejam considerados, para estabelecer modelos-padrão para a configuração segura de *hardware*, *software*, serviços e redes:

a) minimização do número de identidades com direitos privilegiados ou de acesso ao nível do administrador;

b) desabilitação de identidades desnecessárias, não usadas ou inseguras;

c) desabilitação ou restrição de funções e serviços desnecessários;

d) restrição de acesso a programas utilitários com direitos privilegiados e configurações de parâmetros de *host*;

e) relógios sincronizados;

f) alteração de informações de autenticação-padrão do fornecedor, como senhas-padrão imediatamente após a instalação e análise crítica de outros parâmetros importantes relacionados à segurança-padrão;

g) acionamento do recurso de desabilitação automática para o *log off* de dispositivos de computação após um período de inatividade predeterminado;

h) verificação de se os requisitos de licença foram atendidos (ver 5.32).

Gerenciando configurações

Convém que configurações estabelecidas de *hardware*, *software*, serviços e redes sejam registradas e que um registro seja mantido de todas as alterações de configuração. Convém que esses registros sejam armazenados com segurança. Isso pode ser alcançado de várias maneiras, como bancos de dados de configuração ou modelos de configuração.

Convém que as alterações nas configurações sigam o processo de gestão de mudanças (ver 8.32).

Os registros de configuração podem conter, conforme pertinente:

a) titular atualizado ou informações de ponto de contato para o ativo;

b) data da última alteração de configuração;

c) versão do modelo de configuração;

d) relação com configurações de outros ativos.

Monitoramento de configurações

Convém que as configurações sejam monitoradas com um conjunto abrangente de ferramentas de gerenciamento de sistemas (por exemplo, utilitários de manutenção, suporte remoto, ferramentas de gerenciamento corporativo, *software* de cópia de segurança das informações e restauração) e sejam analisadas criticamente de forma regular, para verificar as configurações, avaliar os pontos fortes da senha e avaliar as atividades realizadas. As configurações reais podem ser comparadas com os modelos de destino definidos. Convém que quaisquer desvios sejam abordados, seja pela aplicação automática da configuração de destino definida ou pela análise manual do desvio seguido de ações corretivas.

Outras informações

A documentação para sistemas frequentemente registra detalhes sobre a configuração de *hardware* e *software*.

O *hardening* do sistema é uma parte típica da gestão de configuração.

A gestão de configuração pode ser integrada aos processos de gestão de ativos e ferramentas associadas.

A automação geralmente é mais eficaz para gerenciar a configuração de segurança (por exemplo, usando a infraestrutura como código).

Modelos de configuração e alvos podem ser informações confidenciais e convém que sejam protegidos contra acesso não autorizado em conformidade.

8.10 Exclusão de informações

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade	#Proteger	#Proteção_da_ informação #Legal_e_*compliance*	#Proteção

Controle

Convém que as informações armazenadas em sistemas de informação, dispositivos ou em qualquer outra mídia de armazenamento sejam excluídas quando não forem mais necessárias.

Propósito

Evitar a exposição desnecessária de informações sensíveis e estar em *compliance* com requisitos legais, estatutários, regulamentares e contratuais para a exclusão de informações.

Orientação

Geral

Convém que informações sensíveis não sejam mantidas por mais tempo do que é necessário para reduzir o risco de divulgação indesejável.

Ao excluir informações sobre sistemas, aplicações e serviços, convém que seja considerado o seguinte:

a) selecionar um método de exclusão (por exemplo, sobrescrito eletrônico ou eliminação criptográfica) de acordo com os requisitos de negócios e levando em consideração as leis e os regulamentos relevantes;

b) registrar os resultados da exclusão como evidência;

c) ao usar fornecedores de serviços de exclusão de informações, obter deles evidências de exclusão de informações.

Quando terceiros armazenarem as informações da organização em seu nome, convém que a organização considere a inclusão de requisitos sobre exclusão de informações nos acordos de terceiros para aplicá-los durante e mediante a rescisão de tais serviços.

Métodos de exclusão

De acordo com a política específica de tópicos da organização sobre retenção de dados e levando em consideração a legislação e os regulamentos relevantes, convém que informações confidenciais sejam excluídas quando não forem mais necessárias, por:

a) configuração de sistemas para destruir informações com segurança, quando não forem mais necessárias (por exemplo, após um período definido sujeito à política específica do tópico sobre retenção de dados ou por solicitação de acesso ao assunto);

b) exclusão de versões obsoletas, cópias e arquivos temporários onde quer que estejam localizados;

c) uso de *software* de exclusão aprovado e seguro para excluir permanentemente informações, para ajudar a assegurar que as informações não possam ser recuperadas usando ferramentas forenses ou especializadas;

d) uso de provedores aprovados e certificados de serviços de eliminação segura;

e) uso de mecanismos de descarte apropriados para o tipo de mídia de armazenamento que está sendo descartada (por exemplo desmagnetizando o disco rígido e outros meios de armazenamento magnético).

Convém que, quando os serviços em nuvem forem usados, a organização verifique se o método de exclusão fornecido pelo provedor de serviços em nuvem é aceitável e, se for o caso, convém que a organização use ou solicite que o provedor de serviços em nuvem exclua as informações. Convém que esses processos de exclusão sejam automatizados de acordo com políticas específicas por tema, quando disponíveis e aplicáveis. Dependendo da sensibilidade das informações excluídas, os *logs* podem rastrear ou verificar se esses processos de exclusão aconteceram.

Para evitar a exposição não intencional de informações sensíveis quando o equipamento estiver sendo enviado de volta aos fornecedores, convém que informações sensíveis sejam protegidas removendo armazenamentos auxiliares (por exemplo, discos rígidos) e memória antes que o equipamento deixe as instalações da organização.

Considerando que a exclusão segura de alguns dispositivos (por exemplo, *smartphones*) só pode ser alcançada pela destruição ou pelo uso das funções incorporadas nesses dispositivos (por exemplo, “restaurar configurações de fábrica”), convém que a organização escolha o método apropriado de acordo com a classificação das informações manuseadas por tais dispositivos.

Convém que as medidas de controle descritas em 7.14 sejam aplicadas para destruir fisicamente o dispositivo de armazenamento e excluir simultaneamente as informações que ele contém.

Um registro oficial de exclusão de informações é útil ao analisar a causa de um possível evento de vazamento de informação.

Outras informações

Informações sobre exclusão de dados do usuário em serviços em nuvem podem ser encontradas na ABNT NBR ISO/IEC 27017.

Informações sobre a exclusão de DP podem ser encontradas na ISO/IEC 27555.

8.11 Mascaramento de dados

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade	#Proteger	#Proteção_da_ informação	#Proteção

Controle

Convém que o mascaramento de dados seja usado de acordo com a política específica por tema da organização sobre controle de acesso e outros requisitos específicos por tema relacionados e requisitos de negócios, levando em consideração a legislação aplicável.

Propósito

Limitar a exposição de dados confidenciais, incluindo DP, e cumprir requisitos legais, estatutários, regulamentares e contratuais.

Orientação

Quando a proteção de dados sensíveis (por exemplo, DP) for uma preocupação, convém que as organizações considerem esconder tais dados utilizando técnicas como mascaramento de dados, pseudonimização ou anonimização.

Técnicas de pseudonimização ou anonimização podem ocultar o DP, disfarçar a verdadeira identidade dos titulares de DP ou outras informações sensíveis e desconectar a ligação entre o DP e a identidade do titular do DP ou a ligação entre outras informações sensíveis.

Convém que, ao usar técnicas de pseudonimização ou anonimização, seja verificado se os dados foram adequadamente pseudonimizados ou anonimizados. Convém que a anonimização dos dados considere que todos os elementos das informações sensíveis são eficazes. Como exemplo, se não for considerado adequadamente, uma pessoa pode ser identificada mesmo que os dados que possam identificar diretamente essa pessoa sejam anonimizados, pela presença de mais dados que permitam que a pessoa seja identificada indiretamente.

Técnicas adicionais para mascaramento de dados incluem:

a) criptografia (exigindo que os usuários autorizados tenham uma chave);

b) anulação ou exclusão de caracteres (impedindo que usuários não autorizados vejam mensagens completas);

c) números e datas variados;

d) substituição (alteração de um valor por outro para ocultar dados sensíveis);

e) substituição de valores por seu *hash*.

Convém que sejam consideradas as seguintes técnicas de mascaramento de dados:

a) não conceder a todos os usuários o acesso a todos os dados, projetando consultas e máscaras, a fim de mostrar apenas os dados mínimos necessários ao usuário;

b) há casos em que convém que alguns dados não sejam visíveis ao usuário para alguns registros de um conjunto de dados; neste caso, projetar e implementar um mecanismo de ofuscação de dados (por exemplo, se um paciente não quiser que os funcionários do hospital possam ver todos os seus registros, mesmo em caso de emergência, então a equipe do hospital é apresentada com dados e dados parcialmente ofuscados, e dados só podem ser acessados por funcionários com papéis específicos se contiverem informações úteis para o tratamento adequado);

c) quando os dados são ofuscados, dando ao titular de DP a possibilidade de exigir que os usuários não possam ver se os dados são ofuscados (ofuscação da ofuscação; isso é usado em unidades de saúde, por exemplo, se o paciente não quiser que o pessoal veja que informações sensíveis, como gravidez ou resultados de exames de sangue, foram ofuscadas);

d) quaisquer requisitos legais ou regulamentares (por exemplo, exigindo o mascaramento das informações dos cartões de pagamento durante o tratamento ou armazenamento).

Convém que sejam considerados, ao usar o mascaramento de dados, a pseudonimização ou a anonimização:

a) nível de força de mascaramento de dados, pseudonimização ou anonimização de acordo com o uso dos dados tratados;

b) controles de acesso aos dados tratados;

c) acordos ou restrições ao uso dos dados tratados;

d) proibição de colagem dos dados tratados com outras informações para identificar o titular de DP;

e) acompanhamento do fornecimento e do recebimento dos dados tratados.

Outras informações

A anonimização altera irreversivelmente o DP de tal forma que o titular de DP não pode mais ser identificado direta ou indiretamente.

A pseudonimização substitui as informações de identificação por um pseudônimo. O conhecimento do algoritmo (às vezes referido como “informação adicional”) usado para realizar a pseudonimização permite pelo menos alguma forma de identificação do titular de DP. Convém, portanto, que essas “informações adicionais” sejam mantidas separadas e protegidas.

Embora a pseudonimização seja, portanto, mais fraco que a anonimização, os conjuntos de dados pseudononimizados podem ser mais úteis em pesquisas estatísticas.

O mascaramento de dados é um conjunto de técnicas para ocultar, substituir ou ofuscar itens de dados confidenciais. O mascaramento de dados pode ser estático (quando os itens de dados são mascarados no banco de dados original), dinâmico (usando automação e regras para proteger dados em tempo real) ou em tempo real (com dados mascarados na memória de uma aplicação).

Funções *hash* podem ser usadas para anonimizar os DP. Para evitar ataques de enumeração, convém que eles sejam sempre combinados com uma *salt function.*

Convém que DP em identificadores de recursos e seus atributos [por exemplo, nomes de arquivos, localizadores de recursos uniformes (URL)] sejam evitados ou apropriadamente anonimizados.

Controles adicionais sobre a proteção de DP em nuvens públicas são fornecidos na ABNT NBR ISO/IEC 27018.

Informações adicionais sobre técnicas de desidentificação estão disponíveis na ISO/IEC 20889.

8.12 Prevenção de vazamento de dados

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo #Detectivo	#Confidencialidade	#Proteger #Detectar	#Proteção_da_informação	#Proteção #Defesa

Controle

Convém que medidas de prevenção de vazamento de dados sejam aplicadas a sistemas, redes e quaisquer outros dispositivos que tratem, armazenem ou transmitam informações sensíveis.

Propósito

Detectar e prevenir a divulgação e extração não autorizadas de informações por indivíduos ou sistemas.

Orientação

Convém que a organização considere o seguinte para reduzir o risco de vazamento de dados:

a) identificar e classificar informações para proteger contra vazamentos (por exemplo, informações pessoais, modelos de preços e projetos de produtos);

b) monitorar os canais de vazamento de dados (por exemplo, *e-mails*, transferências de arquivos, dispositivos móveis e dispositivos de armazenamento portáteis);

c) agir de modo a evitar que informações vazem (por exemplo, *e-mails* de quarentena contendo informações sensíveis).

Convém que as ferramentas de prevenção de vazamento de dados sejam usadas para:

a) identificar e monitorar informações sensíveis em risco de divulgação não autorizada (por exemplo, em dados não estruturados no sistema de um usuário);

b) detectar a divulgação de informações sensíveis (por exemplo, quando as informações são enviadas para serviços em nuvem de terceiros não confiáveis ou são enviadas por *e-mail*);

c) bloquear ações de usuários ou transmissões de rede que exponham informações sensíveis (por exemplo, impedindo a cópia de entradas de banco de dados em uma planilha).

Convém que a organização determine se é necessário restringir a capacidade do usuário de copiar e colar ou carregar dados para serviços, dispositivos e mídia de armazenamento fora da organização. Se esse for o caso, convém que a organização implemente tecnologias como ferramentas de prevenção de vazamento de dados ou a configuração de ferramentas existentes que permitam aos usuários visualizar e manipular dados mantidos remotamente, mas evitando copiar e colar fora do controle da organização.

Se for necessária a exportação de dados, convém que o proprietário de dados autorize a aprovação da exportação e mantenha os usuários responsáveis por suas ações.

Convém que a realização de capturas de tela ou fotografias da tela seja abordada por meio de termos e condições de uso, treinamento e auditoria.

Quando os dados forem armazenados em *backup*, convém que seja tomado o cuidado para assegurar que informações sensíveis sejam protegidas, usando medidas como criptografia, controle de acesso e proteção física da mídia de armazenamento que mantenha o *backup*.

Convém que a prevenção de vazamentos de dados também seja considerada para proteger contra as ações de inteligência de um adversário ao obter informações confidenciais ou secretas (geopolítica, humana, financeira, comercial, científica ou qualquer outra) que possam ser de interesse da espionagem

ou possam ser críticas para a comunidade. Convém que as ações de prevenção de vazamento de dados sejam orientadas a confundir as decisões do adversário, por exemplo, substituindo informações autênticas por informações falsas, seja como uma ação independente ou como resposta às ações de inteligência do adversário. Exemplos desse tipo de ações são a engenharia social reversa ou o uso de *honeypots* para atrair atacantes.

Outras informações

As ferramentas de prevenção de vazamento de dados são projetadas para identificar dados, monitorar o uso e a movimentação de dados e tomar medidas para evitar que os dados vazem (por exemplo, alertar os usuários sobre seu comportamento de risco e bloquear a transferência de dados para dispositivos de armazenamento portáteis).

A prevenção de vazamentos de dados envolve, inerentemente, monitorar as comunicações e atividades *online* das pessoas e, por extensão, de mensagens de partes externas, o que levanta preocupações legais que convém que sejam consideradas antes da implantação de ferramentas de prevenção de vazamento de dados. Há uma variedade de legislação relacionada à privacidade, proteção de dados, emprego, interceptação de dados e telecomunicações, que é aplicável ao monitoramento e tratamento de dados no contexto da prevenção de vazamento de dados.

A prevenção de vazamentos de dados pode ser apoiada por controles de segurança-padrão, como políticas específicas por temas no controle de acesso e gerenciamento seguro de documentos (ver 5.12 e 5.15).

8.13 *Backup* das informações

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Corretivo	#Integridade #Disponibilidade	#Recuperar	#Continuidade	#Proteção

Controle

Convém que cópias de *backup* de informações, *software* e sistemas sejam mantidas e testadas regularmente de acordo com a política específica por tema acordada sobre *backup*.

Propósito

Permitir a recuperação da perda de dados ou sistemas.

Orientação

Convém que uma política específica de tema sobre *backup* seja estabelecida para atender aos requisitos de retenção de dados e segurança da informação da organização.

Convém que instalações de *backup* adequadas sejam fornecidas para assegurar que todas as informações e *softwares* essenciais possam ser recuperados após um incidente ou falha ou perda de mídia de armazenamento.

Convém que planos sejam desenvolvidos e implementados sobre como a organização fará cópia de segurança das informações, *software* e sistemas, para abordar a política específica por tema sobre *backup*.

Ao projetar um plano de *backup*, convém que os seguintes itens sejam levados em consideração:

a) produção de registros precisos e completos das cópias de *backup* e procedimentos de restauração documentada;

b) reflexão dos requisitos de negócios da organização (por exemplo, o objetivo do ponto de recuperação – ver 5.30), dos requisitos de segurança das informações envolvidas e da criticidade das informações para o funcionamento contínuo da organização na extensão (por exemplo, *backup* completo ou diferencial) e da frequência de *backups*;

c) armazenamento de *backup* em um local remoto e seguro, a uma distância suficiente para escapar de qualquer dano causado por um desastre no local principal;

d) fornecimento de informações de *backup* com um nível apropriado de proteção física e ambiental (ver a Seção 7 e 8.1), consistente com as normas aplicadas no local principal;

e) teste regular de mídias de *backup* para assegurar que elas possam ser confiadas para uso emergencial, quando necessário. Teste da capacidade de restaurar dados apoiados em um sistema de teste, não substituindo a mídia de armazenamento original no caso de o processo de *backup* ou restauração falhar e causar danos ou perdas irreparáveis de dados;

f) proteção do *backup* por meio da criptografia, de acordo com os riscos identificados (por exemplo, em situações em que a confidencialidade seja importante);

g) cuidado para assegurar que a perda inadvertida de dados seja detectada antes que a *backup* seja tomada.

Convém que os procedimentos operacionais monitorem a execução do *backup* e resolvam falhas dos *backups* programados, para assegurar a integridade dos *backups* de acordo com a política específica por tema sobre *backup*.

Convém que as medidas de *backup* para sistemas e serviços individuais sejam testadas regularmente para assegurar que elas atendam aos objetivos dos planos de resposta a incidentes e continuidade de negócios (ver 5.30). Convém que isto seja combinado com o procedimento de restauração e checado em relação ao tempo de restauração requerido pelo plano de continuidade de negócios. No caso de sistemas e serviços críticos, convém que as medidas de *backup* abranjam todas as informações do sistema, aplicações e dados necessários para recuperar o sistema completo em caso de desastre.

Convém que, quando a organização usar um serviço em nuvem, cópias de *backups* de informações, aplicações e sistemas da organização no ambiente de serviços em nuvem sejam feitas. Convém que a organização determine se e como os requisitos de *backup* são cumpridos ao usar o serviço de *backup* fornecido como parte do serviço em nuvem.

Convém que o período de retenção de informações essenciais do negócio seja determinado, levando em conta qualquer exigência de retenção de cópias de arquivo. Convém que a organização considere a exclusão de informações (ver 8.10) em mídia de armazenamento usada para *backup* assim que o período de retenção das informações expirar, e convém que leve em consideração a legislação e os regulamentos.

Outras informações

Para obter mais informações sobre segurança de armazenamento, incluindo consideração de retenção, ver a ISO/IEC 27040.

8.14 Redundância dos recursos de tratamento de informações

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Disponibilidade	#Proteger	#Continuidade #Gestão_de_ativos	#Proteção #Resiliência

Controle

Convém que os recursos de tratamento de informações sejam implementados com redundância suficiente para atender aos requisitos de disponibilidade.

Propósito

Assegurar o funcionamento contínuo dos recursos de tratamento de informações.

Orientação

Convém que a organização identifique os requisitos para a disponibilidade de serviços de negócios e sistemas de informação. Convém que a organização projete e implemente a arquitetura de sistemas com redundância adequada para atender a esses requisitos.

A redundância pode ser introduzida duplicando os recursos de tratamento de informações em parte ou em sua totalidade (ou seja, componentes sobressalentes ou tendo dois de tudo). Convém que a organização planeje e implemente procedimentos para a ativação dos componentes redundantes e recursos de tratamento. Convém que os procedimentos estabeleçam se os componentes redundantes e as atividades de tratamento estão sempre ativados ou, em caso de emergência, ativados automaticamente ou manualmente. Convém que os componentes redundantes e os recursos de tratamento de informações assegurem o mesmo nível de segurança que os principais.

Convém que os mecanismos estejam em vigor para alertar a organização sobre qualquer falha nos recursos de tratamento de informações e permitam a execução do procedimento planejado e a disponibilidade contínua enquanto os recursos de tratamento de informações são reparadas ou substituídas.

Convém que a organização considere o seguinte ao implementar sistemas redundantes:

a) contratação com dois ou mais fornecedores de recursos de tratamento de informações de rede críticas como provedores de serviços de *internet*;

b) uso de redes redundantes;

c) uso de dois *data centers* geograficamente separados com sistemas espelhados;

d) uso de fornecedores ou fontes de alimentação fisicamente redundantes;

e) uso de várias instâncias paralelas de componentes de *software*, com balanceamento automático de carga entre eles (entre instâncias no mesmo *data center* ou em *data centers* diferentes);

f) componentes duplicados em sistemas (por exemplo, CPU, discos rígidos, memórias) ou em redes (por exemplo, *firewalls*, roteadores, *switches*).

Quando aplicável, preferencialmente no modo de produção, convém que os sistemas de informação redundantes sejam testados para assegurar que a transferência da operação de um componente para outro componente funcione conforme o planejado.

Outras informações

Há uma forte relação entre redundância e prontidão de TIC para a continuidade de negócios (ver 5.30), especialmente se forem necessários tempos curtos de recuperação. Muitas das medidas de redundância podem fazer parte das estratégias e soluções de continuidade da TIC.

A implementação de redundâncias pode introduzir riscos à integridade (por exemplo, processos de cópia de dados para componentes duplicados podem introduzir erros) ou à confidencialidade (por exemplo, o fraco controle de segurança de componentes duplicados pode levar ao comprometimento) das informações e dos sistemas de informação, que precisam ser considerados ao projetar sistemas de informação.

A redundância nos recursos de tratamento de informações geralmente não aborda a indisponibilidade de aplicações devido a falhas dentro de uma aplicação.

Com o uso da computação em nuvem pública, é possível ter várias versões ativas de recursos de tratamento de informações, existentes em vários locais físicos separados com a transferência de operação automático e balanceamento de carga entre eles.

Algumas das tecnologias e técnicas para fornecer redundância e a transferência de operação automática no contexto dos serviços em nuvem são discutidas na ISO/IEC TS 23167.

8.15 *Log*

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Detectivo	#Confidencialidade #Integridade #Disponibilidade	#Detectar	#Gestão_de_eventos_de_segurança_da_informação	#Proteção #Defesa

Controle

Convém que *logs* que registrem atividades, exceções, falhas e outros eventos relevantes sejam produzidos, armazenados, protegidos e analisados.

Propósito

Registrar eventos, gerar evidências, assegurar a integridade das informações de registro, prevenir contra acesso não autorizado, identificar eventos de segurança da informação que possam levar a um incidente de segurança da informação e apoiar investigações.

Orientação

Geral

Convém que a organização determine a finalidade para a qual os *logs* são criados, quais dados são coletados e registrados e quaisquer requisitos específicos para proteger e manusear os dados de *log*. Convém que isso seja documentado em uma política específica por tema sobre l*og*.

Convém que os *logs* de eventos incluam para cada evento, conforme aplicável:

a) ID do usuário;

b) atividades do sistema;

c) datas, horários e detalhes dos eventos relevantes (por exemplo, *log-on* e *log-off*);

d) identidade do dispositivo, identificador do sistema e localização;

e) endereços e protocolos de rede.

Convém que os seguintes eventos sejam considerados para fins de *log*:

a) tentativas de acesso ao sistema bem-sucedidas e rejeitadas;

b) dados bem-sucedidos e rejeitados e outras tentativas de acesso a recursos;

c) alterações na configuração do sistema;

d) uso de privilégios;

e) uso de programas e aplicações utilitários;

f) arquivos acessados e tipo de acesso, incluindo a exclusão de arquivos de dados importantes;

g) alarmes levantados pelo sistema de controle de acesso;

h) ativação e desativação de sistemas de segurança, como sistemas antivírus e sistemas de detecção de intrusão;

i) criação, modificação ou exclusão de identidades;

j) transações executadas pelos usuários em aplicações. Em alguns casos, os aplicações são um serviço ou produto fornecido ou executado por terceiros.

É importante que todos os sistemas tenham fontes de tempo sincronizadas (ver 8.17), pois isso permite correlação de registros entre sistemas para análise, alerta e investigação de um incidente.

Proteção de *logs*

Convém que os usuários, incluindo aqueles com direitos de acesso privilegiados, não tenham permissão para excluir ou desativar *logs* de suas próprias atividades. Eles podem potencialmente manipular os *logs* dos recursos de tratamento de informações que estão sob seu controle direto. Portanto, é necessário proteger e analisar criticamente os *logs* para manter a responsabilização das contas dos usuários privilegiados.

Convém que os controles visem proteger contra mudanças não autorizadas em informações de *log* e de problemas operacionais com os recursos de *log,* incluindo:

a) alterações nos tipos de mensagens que são registrados;

b) arquivos de *log* sendo editados ou excluídos;

c) falha ao gravar eventos ou sobrescrito de eventos gravados passados, se a mídia de armazenamento de um *log* de arquivo for excedida.

Para a proteção de *logs*, convém considerar o uso das seguintes técnicas: *hashing* criptográfico, gravação em um arquivo somente de inclusão e somente leitura, gravação em um arquivo de transparência pública.

Alguns *logs* de auditoria podem ser obrigados a ser arquivados devido a requisitos sobre retenção de dados ou requisitos para coletar e reter evidências (ver 5.28).

Quando a organização precisar enviar *logs* de sistema ou aplicativo para um fornecedor para ajudar a depurar ou solucionar problemas, convém que os *logs* sejam anonimizados, sempre que possível, usando técnicas de mascaramento de dados (ver 8.11) para informações como nomes de usuário, endereços IP, nomes de *host* ou nome da organização, antes de serem enviados ao fornecedor.

Os *logs* de eventos podem conter dados confidenciais e dados pessoais. Convém que a privacidade adequada e as medidas de proteção sejam tomadas (ver 5.34).

Análise de *log*

Convém que a análise de *log* abranja a análise e interpretação de eventos de segurança da informação, para ajudar a identificar atividade incomum ou comportamento anômalo, o que pode representar indicadores de comprometimento.

Convém que a análise dos eventos seja realizada levando em conta:

a) as habilidades necessárias para os especialistas que realizam a análise;

b) a definição do procedimento de análise de *log*;

c) os atributos necessários de cada evento relacionado à segurança;

d) as exceções identificadas pelo uso de regras predeterminadas (por exemplo, regras de gestão da segurança da informação e eventos (SIEM) ou *firewall*, e assinaturas de IDS ou *malware*);

e) os padrões de comportamento conhecidos e de tráfego de rede-padrão em comparação com a atividade e o comportamento anômalos (UEBA);

f) os resultados da análise de tendências ou padrões (por exemplo, como resultado do uso de análise de dados, técnicas de *big data* e ferramentas de análise especializada);

g) a inteligência de ameaças disponível.

Convém que a análise de *log* seja apoiada por atividades específicas de monitoramento para ajudar a identificar e analisar comportamento anômalo, incluindo:

a) analisar criticamente as tentativas bem-sucedidas e malsucedidas de acessar recursos protegidos (por exemplo, servidores de DNS, portais *web* e compartilhamentos de arquivos);

b) verificar registros de DNS para identificar conexões de rede de saída para servidores mal-intencionados, como aqueles associados aos servidores de comando e controle de *botnet*;

c) examinar relatórios de uso de prestadores de serviços (por exemplo, faturas ou relatórios de serviços) para atividades incomuns dentro de sistemas e redes (por exemplo, revisando padrões de atividade);

d) incluir registros de eventos de monitoramento físico, como entrada e saída, para assegurar uma detecção e análise de incidentes mais precisas;

e) correlacionar *logs* para permitir uma análise eficiente e altamente precisa.

Convém que incidentes suspeitos e reais de segurança da informação sejam identificados (por exemplo, infecção por *malware* ou sondagem de *firewalls*) e estejam sujeitos a uma investigação mais aprofundada (por exemplo, como parte de um processo de gestão de incidentes de segurança da informação, ver 5.25).

Outras informações

Os registros do sistema geralmente contêm um grande volume de informações, sendo muitas das quais irrelevantes para o monitoramento de segurança da informação. Para ajudar a identificar eventos significativos para fins de monitoramento de segurança da informação, o uso de programas utilitários adequados ou ferramentas de auditoria para realizar interrogatórios de arquivos pode ser considerado.

O *log* de eventos estabelece as bases para sistemas de monitoramento automatizados (ver 8.16) que são capazes de gerar relatórios consolidados e alertas sobre a segurança do sistema.

Uma ferramenta de gerenciamento de eventos de segurança da informação (SIEM) ou serviço equivalente pode ser usado para armazenar, correlacionar, normalizar e analisar informações de *log* e gerar alertas. Os SIEM tendem a exigir uma configuração cuidadosa para otimizar seus benefícios. As configurações a serem consideradas incluem identificação e seleção de fontes de *log* apropriadas, ajuste e teste de regras e desenvolvimento de casos de uso.

Os arquivos de transparência pública para o registro de *logs* são usados, por exemplo, em sistemas de transparência de certificados. Esses arquivos podem fornecer um mecanismo de detecção adicional útil para proteger contra adulteração de *log*.

Em ambientes em nuvem, as responsabilidades de gerenciamento de *log* podem ser compartilhadas entre o cliente de serviços em nuvem e o provedor de serviços em nuvem. As responsabilidades variam dependendo do tipo de serviço em nuvem que está sendo utilizado. Mais orientações podem ser encontradas na ABNT NBR ISO/IEC 27017.

8.16 Atividades de monitoramento

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Detectivo #Corretivo	#Confidencialidade #Integridade #Disponibilidade	#Detectar #Responder	#Gestão_de_eventos_de_segurança_da_informação	#Defesa

Controle

Convém que redes, sistemas e aplicações sejam monitorados por comportamentos anômalos e por ações apropriadas, tomadas para avaliar possíveis incidentes de segurança da informação.

Propósito

Detectar comportamentos anômalos e possíveis incidentes de segurança da informação.

Orientação

Convém que o escopo e o nível de monitoramento sejam determinados de acordo com os requisitos de segurança do negócio e da informação, e levando em consideração leis e regulamentos relevantes. Convém que os registros de monitoramento sejam mantidos para períodos de retenção definidos.

Convém que sejam considerados para inclusão no sistema de monitoramento:

a) tráfego de rede de saída e entrada, sistema e aplicativo;

b) acesso a sistemas, servidores, equipamentos de rede, sistema de monitoramento, aplicações críticas etc.

c) arquivos críticos ou de nível administrativo e de configuração de rede;

d) *logs* de ferramentas de segurança [por exemplo, antivírus, IDS, sistema de prevenção de intrusão (IPS), filtros *web*, *firewalls*, prevenção de vazamento de dados];

e) *logs* de eventos relacionados à atividade do sistema e da rede;

f) verificação que o código que está em execução está autorizado a ser executado no sistema e que ele não foi adulterado (por exemplo, por recompilação para adicionar código indesejado adicional);

g) uso dos recursos (por exemplo, CPU, discos rígidos, memória, largura de banda) e seu desempenho.

Convém que a organização estabeleça uma linha de base de comportamento normal e monitore esta linha de base para anomalias. Ao estabelecer uma linha de base, convém que seja considerado o seguinte:

a) análise crítica da utilização de sistemas em períodos normais e de pico;

b) tempo habitual de acesso, local de acesso, frequência de acesso para cada usuário ou grupo de usuários.

Convém que o sistema de monitoramento seja configurado contra a linha de base estabelecida para identificar comportamentos anômalos, como:

a) rescisão não planejada de processos ou aplicações;

b) atividade tipicamente associada a *malware* ou tráfego originário de endereços IP maliciosos conhecidos ou domínios de rede (por exemplo, aqueles associados aos servidores de comando e controle de *botnet*);

c) características de ataque conhecidas (por exemplo, negação de serviço e *buffer overflows*);

d) comportamento incomum do sistema (por exemplo, registro de teclas, injeção de processo e desvios no uso de protocolos-padrão);

e) gargalos e sobrecargas (por exemplo, fila de rede, níveis de latência e instabilidade de rede);

f) acesso não autorizado (real ou tentativo) a sistemas ou informações;

g) digitalização não autorizada de aplicações, sistemas e redes de negócios;

h) tentativas bem-sucedidas e malsucedidas de acessar recursos protegidos (por exemplo, servidores DNS, portais *web* e sistemas de arquivos);

i) comportamento incomum do usuário e do sistema em relação ao comportamento esperado.

Convém que seja utilizado o monitoramento contínuo por meio de uma ferramenta de monitoramento. Convém que o monitoramento seja feito em tempo real ou em intervalos periódicos, sujeitos à necessidade organizacional e às capacidades. Convém que as ferramentas de monitoramento incluam a capacidade de lidar com grandes quantidades de dados, adaptar-se a um cenário de ameaças em constante mudança e permitir uma notificação em tempo real. Convém que as ferramentas também sejam capazes de reconhecer assinaturas específicas e dados ou padrões de comportamento de rede ou aplicações.

Convém que o *software* de monitoramento automatizado seja configurado para gerar alertas (por exemplo, por meio de consoles de gerenciamento, mensagens de *e-mail* ou sistemas de mensagens instantâneas) com base em limites predefinidos. Convém que o sistema de alerta seja ajustado e treinado na linha de base da organização para minimizar falsos positivos. Convém que haja pessoal dedicado para responder aos alertas e convém que seja devidamente treinado para interpretar com precisão possíveis incidentes. Convém que haja sistemas e processos redundantes para receber e responder às notificações de alerta.

Convém que eventos anormais sejam comunicados às partes relevantes para melhorar as seguintes atividades: auditoria, avaliação de segurança, varredura e monitoramento de vulnerabilidades (ver 5.25). Convém que os procedimentos sejam realizados para responder a indicadores positivos do sistema de monitoramento em tempo hábil, a fim de minimizar o efeito de eventos adversos (ver 5.26) na segurança da informação. Também convém que sejam estabelecidos procedimentos para identificar e abordar falsos positivos, incluindo o ajuste do *software* de monitoramento, para reduzir o número de futuros falsos positivos.

Outras informações

O monitoramento de segurança pode ser aprimorado por:

a) aproveitamento de sistemas de inteligência de ameaças (ver 5.7);

b) aproveitamento de recursos de aprendizado de máquina e inteligência artificial;

c) uso de listas de bloqueio ou listas de liberação;

d) realização de uma série de avaliações técnicas de segurança (por exemplo, avaliações de vulnerabilidade, testes de penetração, simulações de ataque cibernético e exercícios de resposta cibernética) e uso dos resultados dessas avaliações para ajudar a determinar linhas de base ou comportamento aceitável;

e) uso de sistemas de monitoramento de desempenho para ajudar a estabelecer e detectar comportamentos anômalos;

f) aproveitamento de *logs* em combinação com sistemas de monitoramento.

Muitas vezes, as atividades de monitoramento são realizadas usando *softwares* especializados, como sistemas de detecção de intrusões. Estes podem ser configurados para uma linha de base de atividades normais, aceitáveis e esperadas do sistema e da rede.

O monitoramento de comunicações anômalas ajuda na identificação de *botnets* (ou seja, conjunto de dispositivos sob o controle malicioso do proprietário da *botnet*, geralmente usado para montagem de ataques de negação de serviço distribuídos em outros computadores de outras organizações). Se o computador estiver sendo controlado por um dispositivo externo, há uma comunicação entre o dispositivo infectado e o controlador. Convém que a organização, portanto, empregue tecnologias para monitorar as comunicações anômalas e para tomar tais medidas, conforme necessário.

8.17 Sincronização do relógio

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Detecção	#Integridade	#Proteger #Detectar	#Gestão_de_eventos_de_segurança_da_informação	#Proteção #Defesa

Controle

Convém que os relógios dos sistemas de tratamento de informações utilizados pela organização sejam sincronizados com fontes de tempo aprovadas.

Propósito

Permitir a correlação e a análise de eventos relacionadas à segurança e a outros dados registrados, e apoiar investigações sobre incidentes de segurança da informação.

Orientação

Convém que os requisitos externos e internos para representação do tempo, sincronização confiável e precisão sejam documentados e implementados. Tais requisitos podem ser de necessidades legais, estatutárias, regulamentares, contratuais, de normas e de monitoramento interno. Convém que um tempo de referência padrão seja definido para uso dentro da organização e considerado para todos os sistemas, incluindo sistemas de gerenciamento de edifícios, sistemas de entrada e saída e outros que possam ser usados para auxiliar as investigações.

Convém que um relógio ligado a um relógio atômico nacional por transmissão de rádio ou sistema de posicionamento global (GPS) seja usado como o relógio de referência para sistemas de registro, com uma fonte de data e hora consistente e confiável para assegurar carimbos de tempo precisos. Convém que protocolos como o protocolo de tempo de rede (NTP) ou o protocolo de tempo de precisão (PTP) sejam usados para manter todos os sistemas em rede em sincronização com um relógio de referência.

A organização pode usar duas fontes de tempo externas ao mesmo tempo, a fim de melhorar a confiabilidade dos relógios externos e gerenciar adequadamente qualquer variação.

A sincronização do relógio pode ser difícil ao se usarem vários serviços de nuvem ou ao se usarem serviços de nuvem e locais. Neste caso, convém que o relógio de cada serviço seja monitorado e a diferença registrada para mitigar riscos decorrentes de discrepâncias.

Outras informações

A configuração correta dos relógios de computador é importante para assegurar a exatidão dos *logs* de eventos, que podem ser necessários para investigações ou como evidência em casos legais e disciplinares. *Logs* de auditoria imprecisos podem dificultar tais investigações e prejudicar a credibilidade de tais evidências.

8.18 Uso de programas utilitários privilegiados

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Segurança_de_sistemas_e_rede #Configuração_segura #Segurança_de_aplicação	#Proteção

Controle

Convém que o uso de programas utilitários que possam ser capazes de substituir os controles de sistema e aplicações seja restrito e rigorosamente controlado.

Propósito

Assegurar que o uso de programas utilitários não prejudique os controles do sistema e das aplicações para a segurança da informação.

Orientação

Convém que as seguintes diretrizes para o uso de programas utilitários que podem ser capazes de substituir o sistema e os controles de aplicação sejam consideradas:

a) limitação do uso de programas utilitários ao número mínimo exequível de usuários autorizados confiáveis (ver 8.2);

b) utilização de procedimentos de identificação, autenticação e autorização para programas utilitários, incluindo identificação exclusiva da pessoa que utiliza o programa utilitário;

c) definição e documentação dos níveis de autorização para programas utilitários;

d) autorização para uso *ad hoc* de programas utilitários;

e) não disponibilização de programas utilitários para usuários que tenham acesso a aplicações em sistemas em que a segregação de funções seja necessária;

f) remoção ou desativação de todos os programas utilitários desnecessários;

g) no mínimo, uma segregação lógica de programas utilitários de *software* de aplicações. Quando prático, segregação de comunicações de rede para tais programas a partir do tráfego de aplicações;

h) limitação da disponibilidade de programas utilitários (por exemplo, no período de duração de uma alteração autorizada);

i) registro de todo o uso de programas utilitários.

Outras informações

A maioria dos sistemas de informação tem um ou mais programas utilitários que podem ser capazes de substituir controles de sistema e aplicações, por exemplo, diagnósticos, *patches*, antivírus, desfragmentadores de disco, depuradores, ferramentas de *backup* e rede.

8.19 Instalação de *software* em sistemas operacionais

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de Segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Configuração_segura #Segurança_de_aplicação	#Proteção

Controle

Convém que procedimentos e medidas sejam implementados para gerenciar com segurança a instalação de *software* em sistemas operacionais.

Propósito

Assegurar a integridade dos sistemas operacionais e evitar a exploração de vulnerabilidades técnicas.

Orientação

Convém que as seguintes diretrizes sejam consideradas para gerenciar com segurança as alterações e a instalação de *software* em sistemas operacionais:

a) realizar atualizações de *software* operacional apenas por administradores treinados com as autorizações apropriadas da direção (ver 8.5);

b) assegurar que apenas o código executável aprovado e não o código de desenvolvimento ou compiladores seja instalado em sistemas operacionais;

c) somente a instalar e atualizar o *software* após testes completos e bem-sucedidos (ver 8.29 e 8.31);

d) atualizar todas as bibliotecas do programa-fonte;

e) utilizar um sistema de controle de configuração para manter o controle de todos os *softwares* operacionais, bem como a documentação do sistema;

f) definir uma estratégia de reversão antes da implementação das alterações;

g) manter um registro de auditoria de todas as atualizações para o *software* operacional;

h) arquivar versões antigas do *software*, juntamente com todas as informações e parâmetros necessários, procedimentos, detalhes de configuração e *software* de suporte como medida de contingência e enquanto o *software* for necessário para ler ou tratar os dados arquivados.

Convém que qualquer decisão de atualização para uma nova versão leve em conta os requisitos de negócios para a alteração e a segurança da versão (por exemplo, a introdução de novas funcionalidades

de segurança da informação ou o número e a gravidade das vulnerabilidades de segurança da informação que afetam a versão atual). Convém que os *patches* de *software* sejam aplicados quando puderem ajudar a remover ou reduzir as vulnerabilidades de segurança da informação (ver 8.8 e 8.19).

O *software* de computador pode contar com *softwares* e pacotes fornecidos externamente (por exemplo, programas de *software* usando módulos hospedados em *sites* externos), sendo conveniente que sejam monitorados e controlados para evitar alterações não autorizadas, pois podem introduzir vulnerabilidades de segurança da informação.

Convém que o *software* fornecido por partes externas para uso em sistemas operacionais seja mantido em um nível apoiado pelo fornecedor. Com o tempo, os fornecedores de *software* deixarão de apoiar versões mais antigas do *software*. Convém que a organização considere os riscos de confiar em *softwares* sem suporte. Convém que o *software* de código aberto usado em sistemas operacionais seja mantido até a sua versão mais recente apropriada. Com o tempo, o código-fonte aberto pode deixar de ser mantido, mas ainda está disponível em um repositório de *software* de código aberto. Também convém que a organização considere os riscos de depender de um *software* de código aberto não mantido, quando usado em sistemas operacionais.

Quando os fornecedores estiverem envolvidos na instalação ou atualização de *software*, convém que o acesso físico ou lógico só seja dado quando necessário e com a devida autorização. Convém que as atividades do fornecedor sejam monitoradas (ver 5.22).

Convém que a organização defina e imponha regras rígidas sobre quais tipos de *software* os usuários podem instalar.

Convém que o princípio do menor privilégio seja aplicado à instalação de *software* em sistemas operacionais. Convém que a organização identifique quais tipos de instalações de *software* são permitidos (por exemplo, atualizações e *patches* de segurança para *softwares* existentes) e quais tipos de instalações são proibidas (por exemplo, *software* que é apenas para uso pessoal e *software* cuja origem em relação a ser potencialmente malicioso é desconhecida ou suspeita). Convém que esses privilégios sejam concedidos com base nas funções dos usuários em causa.

Outras informações

Não há outra informação.

8.20 Segurança de redes

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo #Detectivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger #Detectar	#Segurança_de_sistemas_e_rede	#Proteção

Controle

Convém que redes e dispositivos de rede sejam protegidos, gerenciados e controlados para proteger as informações em sistemas e aplicações.

Propósito

Proteger as informações nas redes e seus recursos de tratamento de informações de suporte contra o comprometimento por rede.

Orientação

Convém que os controles sejam implementados para assegurar a segurança das informações nas redes e para proteger os serviços conectados de acesso não autorizado. Em particular, convém que sejam considerados os seguintes itens:

a) tipo e nível de classificação das informações que a rede pode suportar;

b) estabelecimento de responsabilidades e procedimentos para a gestão de equipamentos e dispositivos de rede;

c) manutenção da documentação atualizada, incluindo diagramas de rede e arquivos de configuração de dispositivos (por exemplo, roteadores, *switches*);

d) separação da responsabilidade operacional das redes das operações dos sistemas de TIC, quando apropriado (ver 5.3);

e) estabelecimento de controles para salvaguardar a confidencialidade e a integridade dos dados que passam por redes públicas, redes de terceiros ou redes sem fio, e para proteger os sistemas e aplicações conectadas (ver 5.22, 8.24, 5.14 e 6.6). Controles adicionais também podem ser necessários para manter a disponibilidade dos serviços de rede e computadores conectados à rede;

f) registro e monitoramento adequados para permitir o registro e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação (ver 8.16 e 8.15);

g) coordenação de perto das atividades de gerenciamento de rede, tanto para otimizar o serviço à organização, quanto para assegurar que os controles sejam aplicados de forma consistente em toda a infraestrutura de tratamento de informações;

h) sistemas de autenticação na rede;

i) restrição e filtragem da conexão dos sistemas à rede (por exemplo, usando *firewalls*);

j) detecção, restrição e autenticação da conexão de equipamentos e dispositivos à rede;

k) *hardening* de dispositivos de rede;

l) segregação de canais de administração de rede de outros tráfegos de rede;

m) isolamento temporário de sub-redes críticas (por exemplo, com desconexões temporárias), se a rede estiver sob ataque;

n) desativação de protocolos de rede vulneráveis.

Convém que a organização assegure que os controles de segurança apropriados sejam aplicados ao uso de redes virtualizadas. As redes virtualizadas também abrangem redes definidas por *software* (SDN, SD-WAN). As redes virtualizadas podem ser desejáveis do ponto de vista da segurança, pois

podem permitir a separação lógica da comunicação que ocorre em redes físicas, especialmente para sistemas e aplicações que são implementadas por meio da computação distribuída.

Outras informações

Podem ser encontradas informações adicionais sobre segurança de rede na série ISO/IEC 27033.

Mais informações sobre redes virtualizadas podem ser encontradas na ISO/IEC TS 23167.

8.21 Segurança dos serviços de rede

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Segurança_de_sistemas_e_rede	#Proteção

Controle

Convém que sejam identificados, implementados e monitorados mecanismos de segurança, níveis de serviço e requisitos de serviços de rede.

Propósito

Assegurar a segurança no uso de serviços de rede.

Orientação

Convém que sejam identificadas e implementadas as medidas de segurança necessárias para determinados serviços, como recursos de segurança, níveis de serviço e requisitos de serviço (por provedores de serviços de rede internos ou externos). Convém que a organização assegure que os provedores de serviços de rede implementem essas medidas.

Convém que a capacidade do provedor de serviços de rede de gerenciar serviços acordados de forma segura seja determinada e monitorada regularmente. Convém que o direito à auditoria seja acordado entre a organização e o provedor. Convém também que a organização considere atestados de terceiros fornecidos pelos provedores de serviços para demonstrar que mantêm as medidas de segurança adequadas.

Convém que as regras sobre o uso de redes e serviços de rede sejam formuladas e implementadas para abranger:

a) as redes e os serviços de rede que podem ser acessados;

b) os requisitos de autenticação para acessar vários serviços de rede;

c) os procedimentos de autorização para determinar a quem é permitido acessar quais redes e serviços de rede;

d) o gerenciamento de rede e procedimentos e controles tecnológicos para proteger o acesso às conexões de rede e serviços de rede;

e) os meios utilizados para acessar redes e serviços de rede [por exemplo, uso de rede virtual privada (VPN) ou rede sem fio];

f) o tempo, a localização e outros atributos do usuário no momento do acesso;

g) o monitoramento do uso de serviços de rede.

Convém que os seguintes recursos de segurança dos serviços de rede sejam considerados:

a) tecnologia aplicada à segurança de serviços de rede, como autenticação, criptografia e controles de conexão de rede;

b) parâmetros técnicos necessários para a conexão segura com os serviços de rede, de acordo com as regras de segurança e conexão de rede;

c) *cache* (por exemplo, em uma rede de entrega de conteúdo) e seus parâmetros, que permitem aos usuários escolher o uso de cache de acordo com os requisitos de desempenho, disponibilidade e confidencialidade;

d) procedimentos para o uso do serviço de rede para restringir o acesso a serviços ou aplicações de rede, quando necessário.

Outras informações

Os serviços de rede incluem a prestação de conexões, serviços de rede privada e soluções gerenciadas de segurança de rede, como *firewalls* e sistemas de detecção de intrusões. Esses serviços podem variar desde um serviço não gerenciado de provimento de banda até ofertas complexas com alto valor agregado.

Mais orientações sobre uma estrutura para gestão de acesso são dadas na ISO/IEC 29146.

8.22 Segregação de redes

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Segurança_de_sistemas_e_rede	#Proteção

Controle

Convém que grupos de serviços de informação, usuários e sistemas de informação sejam segregados nas redes da organização.

Propósito

Dividir a rede em perímetros de segurança e controlar o tráfego entre eles com base nas necessidades de negócios.

Orientação

Convém que a organização considere gerenciar a segurança de grandes redes dividindo-as em domínios de rede separados e separando-os da rede pública (ou seja, *internet*). Os domínios podem ser escolhidos com base em níveis de confiança, criticidade e sensibilidade (por exemplo, domínio de acesso público, domínio de *desktop*, domínio do servidor, sistemas de baixo e alto riscos), com base em unidades organizacionais (por exemplo, recursos humanos, finanças, *marketing*) ou alguma combinação (por exemplo, domínio de servidor conectando-se a várias unidades organizacionais). A segregação pode ser feita usando redes fisicamente diferentes ou usando diferentes redes lógicas.

Convém que o perímetro de cada domínio seja bem definido. Se o acesso entre domínios de rede for permitido, convém que ele seja controlado no perímetro usando um *gateway* (por exemplo, *firewall*, roteador filtrante). Convém que os critérios de segregação de redes em domínios e o acesso permitido pelos *gateways* sejam baseados em uma avaliação dos requisitos de segurança de cada domínio. Convém que a avaliação esteja de acordo com a política específica por tema sobre controle de acesso (ver 5.15), requisitos de acesso, valor e classificação de informações tratadas, e que leve em conta o impacto relativo de custo e desempenho da incorporação de tecnologia de *gateway* adequada.

As redes sem fio requerem tratamento especial devido ao perímetro de rede mal definido. Convém que o ajuste da cobertura de rádio seja considerado para a segregação de redes sem fio. Para ambientes sensíveis, convém que todo o acesso sem fio seja considerado como conexão externa e que este acesso seja segregado de redes internas até que o acesso passe por um *gateway* de acordo com os controles de rede (ver 8.20), antes de conceder acesso a sistemas internos. Convém que a rede de acesso sem fio para convidados seja separada daquelas para pessoal interno, se o pessoal interno usar apenas *endpoints* com controle de usuário em conformidade com as políticas específicas por tema da organização. Convém que o *wi-fi* para visitantes tenha pelo menos as mesmas restrições que o *wi-fi* para o pessoal interno, a fim de desencorajar o uso de *wi-fi* de visitantes pelo pessoal interno.

Outras informações

Muitas vezes, as redes vão além dos limites organizacionais, à medida que são formadas parcerias comerciais que requerem a interconexão ou o compartilhamento de recursos de tratamento de informações e redes. Essas extensões podem aumentar o risco de acesso não autorizado aos sistemas de informação da organização que usam a rede, e alguns dos quais requerem proteção de outros usuários da rede devido à sua sensibilidade ou criticidade.

8.23 Filtragem da *web*

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Segurança_de_sistemas_e_rede	#Proteção

Controle

Convém que o acesso a *sites* externos seja gerenciado para reduzir a exposição a conteúdo malicioso.

Propósito

Proteger os sistemas de serem comprometidos por *malware* e impedir o acesso a recursos *web* não autorizados.

Orientação

Convém que a organização reduza os riscos de seu pessoal acessar *sites* que contenham informações ilegais ou que sejam conhecidos por conter vírus ou material de *phishing*. Uma técnica para conseguir isso funciona bloqueando o endereço IP ou o domínio do *site* em questão. Alguns navegadores e tecnologias anti-*malware* fazem isso automaticamente ou podem ser configurados para fazê-lo.

Convém que a organização identifique os tipos de *sites* aos quais o seu pessoal pode ou não ter acesso. Convém que a organização considere bloquear o acesso aos seguintes tipos de *sites*:

a) *sites* que possuem uma função de *upload* de informações, a menos que seja permitido por razões comerciais válidas;

b) *sites* maliciosos conhecidos ou suspeitos (por exemplo, aqueles que distribuem conteúdo de *malware* ou *phishing*);

c) servidores de comando e controle;

d) *site* malicioso adquirido a partir de inteligência de ameaças (ver 5.7);

e) *sites* que compartilhem conteúdo ilegal.

Antes de implantar esse controle, convém que as organizações estabeleçam regras para o uso seguro e adequado de recursos *on-line*, incluindo qualquer restrição a *sites* indesejáveis ou inadequados e aplicações baseadas na *web*. Convém que as regras sejam mantidas atualizadas.

Convém que um treinamento seja dado ao pessoal sobre o uso seguro e adequado de recursos *on-line*, incluindo acesso à *web*. Convém que o treinamento inclua as regras da organização, ponto de contato para levantar preocupações de segurança e processo de exceção quando recursos restritos da *web* precisarem ser acessados por razões comerciais legítimas. Convém também que o treinamento seja dado ao pessoal para assegurar que eles não sobrepassem qualquer aviso do navegador que informe que um *site* não é seguro, mas permite que o usuário prossiga.

Outras informações

A filtragem da *web* pode incluir uma série de técnicas, incluindo assinaturas, heurísticas, lista de *sites* ou domínios aceitáveis, lista de *sites* ou domínios proibidos e configuração sob medida para ajudar a evitar que *softwares* maliciosos e outras atividades maliciosas ataquem a rede e os sistemas da organização.

8.24 Uso de criptografia

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Configuração_segura	#Proteção

Controle

Convém que sejam definidas e implementadas regras para o uso efetivo da criptografia, incluindo o gerenciamento de chaves criptográficas.

Propósito

Assegurar o uso adequado e eficaz da criptografia para proteger a confidencialidade, autenticidade ou integridade das informações de acordo com os requisitos de segurança das empresas e da informação, e levando em consideração os requisitos legais, estatutários, regulamentares e contratuais relacionados à criptografia.

Orientação

Geral

Ao usar criptografia, convém que seja considerado o seguinte:

a) a política específica por tema sobre criptografia definida pela organização, incluindo os princípios gerais para a proteção das informações. Uma política específica por tema sobre o uso de criptografia é necessária para maximizar os benefícios e minimizar os riscos do uso de técnicas criptográficas e evitar seu uso inadequado ou incorreto;

b) identificação do nível de proteção necessário e classificação das informações e, consequentemente, estabelecimento do tipo, da força e da qualidade dos algoritmos criptográficos necessários;

c) uso de criptografia para proteção de informações mantidas em *endpoints* móveis do usuário ou mídia de armazenamento e transmitidas por redes para tais dispositivos ou mídia de armazenamento;

d) abordagem do gerenciamento de chaves, incluindo métodos para lidar com a geração e proteção de chaves criptográficas e com a recuperação de informações criptografadas no caso de chaves perdidas, comprometidas ou danificadas;

e) papéis e responsabilidades para:

   1) implementação das regras para o uso efetivo da criptografia;

   2) gerenciamento de chaves, incluindo a geração das chaves (ver 8.24);

f) normas a serem adotadas, bem como algoritmos criptográficos, força da criptografia, soluções criptográficas e práticas de uso que são aprovadas ou necessárias para uso na organização;

g) impacto do uso de informações criptografadas em controles que dependam da inspeção de conteúdo (por exemplo, detecção de *malware* ou filtragem de conteúdo).

Convém que, ao implementar as regras da organização para o uso efetivo da criptografia, os regulamentos e as restrições nacionais que podem se aplicar ao uso de técnicas criptográficas em diferentes partes do mundo sejam levados em consideração, bem como as questões do fluxo transfronteiriço de informações criptografadas (ver 5.31).

Convém que o conteúdo de contratos ou acordos de nível de serviço com fornecedores externos de serviços criptográficos (por exemplo, com autoridade de certificação) abranja questões de responsabilidade, confiabilidade dos serviços e tempos de resposta para a prestação de serviços (ver 5.22).

Gerenciamento de chaves

O gerenciamento adequado de chaves requer processos seguros para gerar, armazenar, arquivar, recuperar, distribuir, retirar e destruir chaves criptográficas.

Convém que um sistema de gerenciamento de chaves seja baseado em um conjunto acordado de padrões, procedimentos e métodos seguros para:

a) gerar chaves para diferentes sistemas criptográficos e diferentes aplicações;

b) emitir e obter certificados de chave pública;

c) distribuir chaves para entidades pretendidas, incluindo como ativar chaves quando recebidas;

d) armazenar chaves, incluindo como os usuários autorizados obtêm acesso às chaves;

e) alterar ou atualizar chaves, incluindo regras sobre quando alterar chaves e como isso será feito;

f) lidar com chaves comprometidas;

g) revogar chaves, incluindo como retirar ou desativar chaves [por exemplo, quando as chaves foram comprometidas ou quando um usuário deixar uma organização (nesse caso, convém que as chaves também sejam arquivadas)];

h) recuperar chaves que são perdidas ou corrompidas;

i) *backup* ou arquivamento de chaves;

j) destruir chaves;

k) registrar e auditar as principais atividades relacionadas à gestão;

l) definir datas de ativação e desativação para chaves, para que as chaves só possam ser usadas pelo período de tempo estabelecido conforme as regras da organização sobre gerenciamento de chaves;

m) lidar com pedidos legais de acesso a chaves criptográficas (por exemplo, informações criptografadas podem ser necessárias para serem disponibilizadas de forma não criptografada como evidência em um processo judicial).

Convém que todas as chaves criptográficas sejam protegidas contra modificações e perdas. Além disso, chaves secretas e privadas precisam de proteção contra uso não autorizado, bem como divulgação. Convém que os equipamentos usados para gerar, armazenar e arquivar chaves sejam protegidos fisicamente.

Além da integridade, convém, para muitos casos de uso, que a autenticidade das chaves públicas também seja considerada.

Outras informações

A autenticidade das chaves públicas geralmente é abordada por processos públicos de gerenciamento de chaves usando autoridades de certificação e certificados de chaves públicas, mas também é possível endereçá-las usando tecnologias como a aplicação de processos manuais para um pequeno número de chaves.

A criptografia pode ser usada para alcançar diferentes objetivos de segurança da informação, por exemplo:

a) confidencialidade: usar criptografia de informações para proteger informações confidenciais ou críticas, armazenadas ou transmitidas;

b) integridade ou autenticidade: usar assinaturas digitais ou códigos de autenticação de mensagens para verificar a autenticidade ou integridade de informações confidenciais ou críticas armazenadas ou transmitidas. Utilizar e algoritmos com o propósito de verificação da integridade de arquivos;

c) não repúdio: utilizar técnicas criptográficas para comprovar a ocorrência ou não ocorrência de um evento ou ação;

d) autenticação: usar técnicas criptográficas para autenticar usuários e outras entidades do sistema, solicitando acesso a ou transacionando com usuários, entidades e recursos do sistema.

A série ISO/IEC 11770 fornece mais informações sobre o gerenciamento de chaves.

8.25 Ciclo de vida de desenvolvimento seguro

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Segurança_de_aplicação #Segurança_de_sistemas_e_rede	#Proteção

Controle

Convém que regras para o desenvolvimento seguro de *software* e sistemas sejam estabelecidas e aplicadas.

Propósito

Assegurar que a segurança da informação seja projetada e implementada dentro do ciclo de vida de desenvolvimento seguro de *software* e sistemas.

Orientação

O desenvolvimento seguro é um requisito para construir serviço, arquitetura, *software* e sistema seguros. Para isso, convém que sejam considerados os seguintes aspectos:

a) separação dos ambientes de desenvolvimento, teste e produção (ver 8.31);

b) orientação sobre a segurança no ciclo de vida do desenvolvimento de *software*:

   1) segurança na metodologia de desenvolvimento de *software* (ver 8.28 e 8.27);

   2) diretrizes de codificação seguras para cada linguagem de programação utilizada (ver 8.28);

c) requisitos de segurança na fase de especificação e *design* (ver 5.8);

d) pontos de verificação de segurança em projetos (ver 5.8);

e) testes de sistema e segurança, como testes de regressão, verificação de código e testes de invasão (ver 8.29);

f) repositórios seguros para código-fonte e configuração (ver 8.4 e 8.9);

g) segurança no controle de versão (ver 8.32);

h) conhecimento e treinamento necessários de segurança de aplicações (ver 8.28);

i) capacidade dos desenvolvedores para prevenir, encontrar e corrigir vulnerabilidades (ver 8.28);

j) requisitos e alternativas de licenciamento para assegurar soluções econômicas, evitando futuros problemas de licenciamento (Ver 5.32).

Se o desenvolvimento for terceirizado, convém que a organização obtenha a garantia de que o fornecedor está de acordo com as regras da organização para o desenvolvimento seguro (ver 8.30).

Outras informações

O desenvolvimento também pode ocorrer aplicações internas, como aplicações de escritório, *scripting*, navegadores e bases de dados.

8.26 Requisitos de segurança da aplicação

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Segurança_de_aplicação #Segurança_de_sistemas_e_rede	#Proteção #Defesa

Controle

Convém que os requisitos de segurança da informação sejam identificados, especificados e aprovados ao desenvolver ou adquirir aplicações.

Propósito

Assegurar que todos os requisitos de segurança da informação sejam identificados e abordados ao desenvolver ou adquirir aplicações.

Orientação

Geral

Convém que os requisitos de segurança de aplicações sejam identificados e especificados. Esses requisitos geralmente são determinados por meio de uma avaliação de risco. Convém que os requisitos sejam desenvolvidos com o apoio de especialistas em segurança da informação.

Os requisitos de segurança de aplicações podem abranger uma ampla gama de tópicos, dependendo do propósito da aplicação.

Convém que os requisitos de segurança de aplicações incluam, conforme aplicável:

a) nível de confiança na identidade das entidades [por exemplo, por meio da autenticação (ver 5.17, 8.2 e 8.5)];

b) identificação do tipo de informação e do nível de classificação a serem tratados pela aplicação;

c) necessidade de segregação de acesso e nível de acesso a dados e funções na aplicação;

d) resiliência contra ataques maliciosos ou disrupções não intencionais [por exemplo, proteção contra *buffer overflow* ou SQL *injections* [inserções de linguagem estruturada de consulta (SQL)];

e) requisitos legais, estatutários e regulamentares na jurisdição onde a transação é gerada, processada, concluída ou armazenada;

f) necessidade de privacidade associada a todas as partes envolvidas;

g) requisitos de proteção de quaisquer informações confidenciais;

h) proteção de dados enquanto são tratados, em trânsito e em repouso;

i) necessidade de criptografar com segurança as comunicações entre todas as partes envolvidas;

j) controles de entrada, incluindo verificações de integridade e validação de entrada;

k) controles automatizados (por exemplo, limites de aprovação ou aprovações duplas);

l) controles de saída, considerando também quem pode acessar as saídas e sua autorização;

m) restrições em torno do conteúdo de campos de “texto livre”, pois estes podem levar ao armazenamento descontrolado de dados confidenciais (por exemplo, dados pessoais);

n) requisitos derivados do processo de negócios, como registro e monitoramento de transações, requisitos de não repúdio;

o) requisitos exigidos por outros controles de segurança (por exemplo, interfaces para sistemas de registro e monitoramento ou detecção de vazamento de dados);

p) manuseio de mensagens de erro.

Serviços transacionais

Além disso, para aplicações que oferecem serviços transacionais entre a organização e um parceiro, convém que o seguinte seja considerado ao se identificarem requisitos de segurança da informação:

a) nível de confiança que cada parte requer em cada identidade declarada pela outra parte;

b) nível de confiança exigido na integridade das informações trocadas ou tratadas e mecanismos de identificação da falta de integridade (por exemplo, verificação de redundância cíclica, *hashing*, assinaturas digitais);

c) processos de autorização associados a quem pode aprovar conteúdos, emitir ou assinar documentos transacionais importantes;

d) confidencialidade, integridade, comprovante de expedição e recebimento de documentos-chave e não repúdio (por exemplo, contratos associados a processos licitatórios e contratuais);

e) confidencialidade e integridade de quaisquer transações (por exemplo, pedidos, detalhes do endereço de entrega e confirmação de recibos);

f) requisitos sobre quanto tempo para manter a transação confidencial;

g) seguro e outros requisitos contratuais.

Pedidos eletrônicos e aplicações de pagamentos

Além disso, para aplicações envolvendo pedidos eletrônicos e pagamento, convém que o seguinte seja considerado:

a) requisitos para manter a confidencialidade e integridade das informações das ordens de pagamento;

b) grau de verificação adequado para verificar as informações de pagamento fornecidas por um cliente;

c) evitamento de perdas ou duplicação de informações de transação;

d) armazenamento de detalhes de transações fora de qualquer ambiente acessível ao público (por exemplo, em uma plataforma de armazenamento existente na *intranet* organizacional, e não retido e exposto em mídia de armazenamento eletrônico diretamente acessível da *internet*);

e) quando uma autoridade confiável é usada (por exemplo, para fins de emissão e manutenção de assinaturas digitais ou certificados digitais), a segurança é integrada e incorporada durante todo o processo de gerenciamento de certificados ou assinaturas de ponta a ponta.

Várias considerações acima podem ser abordadas pela aplicação da criptografia (ver 8.24), levando em consideração os requisitos legais (ver 5.31 a 5.36, especialmente 5.31 para a legislação de criptografia).

Outras informações

As aplicações acessíveis por redes estão sujeitas a uma série de ameaças relacionadas à rede, como atividades fraudulentas, disputas contratuais ou divulgação de informações ao público; transmissão incompleta, roteamento errado, alteração não autorizada de mensagem, duplicação ou repetição. Portanto, processos de avaliação de risco detalhados e determinação cuidadosa dos controles são indispensáveis. Os controles necessários muitas vezes incluem métodos criptográficos para autenticação e proteção da transferência de dados.

Mais informações sobre a segurança de aplicações podem ser encontradas na série ISO/IEC 27034.

8.27 Princípios de arquitetura e engenharia de sistemas seguros

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Segurança_de_aplicação #Segurança_de_sistemas_e_rede	#Proteção

Controle

Convém que princípios de engenharia para sistemas de segurança sejam estabelecidos, documentados, mantidos e aplicados a qualquer atividade de desenvolvimento de sistemas.

Propósito

Assegurar que os sistemas de informação sejam projetados, implementados e operados com segurança dentro do ciclo de vida de desenvolvimento.

Orientação

Convém que os princípios de engenharia de segurança sejam estabelecidos, documentados e aplicados às atividades de engenharia do sistema de informação. Convém que a segurança seja projetada em todas as camadas de arquitetura (negócios, dados, aplicações e tecnologia). Convém que novas tecnologias sejam analisadas com relação aos riscos de segurança e que o *design* seja analisado criticamente em relação aos padrões de ataque conhecidos.

Princípios de engenharia seguros fornecem orientação sobre técnicas de autenticação do usuário, controle de sessão segura e validação de dados e higienização.

Convém que os princípios de engenharia de sistemas seguros incluam a análise de:

a) toda a gama de controles de segurança necessários para proteger as informações e os sistemas contra ameaças identificadas;

b) capacidades dos controles de segurança para prevenir, detectar ou responder a eventos de segurança;

c) controles de segurança específicos requeridos por determinados processos de negócios (por exemplo, criptografia de informações sensíveis, verificação de integridade e assinatura digital de informações);

d) onde e como os controles de segurança devem ser aplicados (por exemplo, integrando-se a uma arquitetura de segurança e à infraestrutura técnica);

e) como os controles de segurança individuais (manuais e automatizados) trabalham juntos para produzir um conjunto de controles integrado.

Convém que os princípios de engenharia de segurança levem em conta:

a) necessidade de se integrar com uma arquitetura de segurança;

b) infraestrutura técnica de segurança [por exemplo, infraestrutura de chaves públicas (PKI), gerenciamento de identidade e acesso (IAM), prevenção de vazamentos de dados e gerenciamento dinâmico de acesso];

c) capacidade da organização para desenvolver e apoiar a tecnologia escolhida;

d) custo, tempo e complexidade para atender aos requisitos de segurança;

e) boas práticas atuais.

Convém que a engenharia segura do sistema envolva:

a) uso de princípios de arquitetura de segurança, como “segurança por *design*”, “defesa em profundidade”, “segurança por padrão”, “negar por padrão”, “falhar com segurança”, “desconfiar de entrada de aplicações externas”, “segurança na implantação”, “assumir violação”, “menor privilégio”, “usabilidade e capacidade de gerenciamento” e “menor funcionalidade”;

b) uma análise crítica de *design* orientada à segurança para ajudar a identificar vulnerabilidades de segurança da informação e assegurar que os controles de segurança sejam especificados e atendam aos requisitos de segurança;

c) documentação e reconhecimento formal de controles de segurança que não atendam totalmente aos requisitos (por exemplo, devido aos requisitos de segurança sobrepostos);

d) *hardening* de sistemas.

Convém que a organização considere os princípios de “confiança zero”, como:

a) assumir que os sistemas de informação da organização já estão violados e, portanto, não depender apenas da segurança do perímetro de rede;

b) empregar uma abordagem “nunca confie e sempre verifique” para o acesso aos sistemas de informação;

c) assegurar que as solicitações aos sistemas de informação sejam criptografadas de ponta a ponta;

d) verificar cada solicitação a um sistema de informações, como se tivesse se originado de uma rede aberta e externa, mesmo que essas solicitações se originem internamente à organização (ou seja, não confiar automaticamente em nada dentro ou fora de seus perímetros);

e) utilizar técnicas de controle de acesso “menos privilegiado” e dinâmica (ver 5.15, 5.18 e 8.2). Isso inclui autenticar e autorizar solicitações de informações ou sistemas baseados em informações contextuais, como informações de autenticação (ver 5.17), identidades do usuário (ver 5.16), dados sobre o *endpoint* do usuário e classificação de dados (ver 5.12);

f) sempre autenticar solicitantes e sempre validar solicitações de autorização para sistemas de informação com base em informações, incluindo informações de autenticação (ver 5.17) e identidades do usuário (5.16), dados sobre o *endpoint* do usuário e classificação de dados (ver 5.12), por exemplo, aplicar autenticação forte (por exemplo, por múltiplos, ver 8.5).

Convém que os princípios estabelecidos de engenharia de segurança sejam aplicados, quando aplicável, ao desenvolvimento terceirizado de sistemas de informação por meio dos contratos e outros acordos vinculativos entre a organização e o fornecedor a quem a organização terceiriza. Convém que a organização assegure que as práticas de engenharia de segurança dos fornecedores estejam alinhadas com as necessidades da organização.

Convém que os princípios de engenharia de segurança e os procedimentos de engenharia estabelecidos sejam regularmente analisados criticamente para assegurar que eles estejam efetivamente contribuindo para o aprimoramento dos padrões de segurança dentro do processo de engenharia. Convém também que eles sejam regularmente analisados criticamente para assegurar que permaneçam atualizados em termos de combate a quaisquer novas ameaças potenciais e para permanecer aplicáveis aos avanços nas tecnologias e soluções que estão sendo aplicadas.

Outras informações

Princípios de engenharia segura podem ser aplicados ao projeto ou à configuração de uma série de técnicas, como:

— tolerância a falhas e outras técnicas de resiliência;

— segregação (por exemplo, por meio de virtualização ou conteinerização);

— resistência a adulteração.

Técnicas seguras de virtualização podem ser usadas para evitar interferências entre aplicações em execução no mesmo dispositivo físico. Se uma instância virtual de uma aplicação for comprometida por um invasor, apenas essa instância será afetada. O ataque não tem efeito em qualquer outro aplicativo ou dados.

Técnicas de resistência a adulteração podem ser usadas para detectar adulteração de contêineres de informações, seja físico (por exemplo, um alarme de roubo) ou lógico (por exemplo, um arquivo de dados). Uma característica de tais técnicas é que há um registro da tentativa de adulteração do contêiner. Além disso, o controle pode impedir a extração bem-sucedida de dados por meio de sua destruição (por exemplo, a memória do dispositivo pode ser excluída).

8.28 Codificação segura

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Segurança_de_aplicação #Segurança_de_sistemas_e_rede	#Proteção

Controle

Convém que princípios de codificação segura sejam aplicados ao desenvolvimento de *software*.

Propósito

Assegurar que o *software* seja escrito com segurança, reduzindo assim o número de potenciais vulnerabilidades de segurança da informação no *software*.

Orientação

Geral

Convém que a organização estabeleça processos em toda a organização para fornecer uma boa governança para uma codificação segura. Convém que uma linha de base segura mínima seja estabelecida e aplicada. Além disso, convém que tais processos e governança sejam estendidos para abranger componentes de *software* de terceiros e *software* de código aberto.

Convém que a organização monitore ameaças do mundo real e conselhos e informações atualizados sobre vulnerabilidades de *software,* para orientar seus princípios de codificação segura por meio da

melhoria e do aprendizado contínuos. Isso pode ajudar a assegurar que práticas eficazes de codificação segura sejam implementadas para combater o cenário de ameaças em rápida mudança.

Planejamento e antes da codificação

Convém que princípios de codificação segura sejam usados tanto em novos desenvolvimentos quanto em cenários de reutilização. Convém que estes princípios sejam aplicados às atividades de desenvolvimento tanto dentro da organização quanto em produtos e serviços fornecidos por ela a terceiros. Convém que o planejamento e os pré-requisitos antes da codificação incluam:

a) expectativas específicas da organização e princípios aprovados para codificação segura a serem usados tanto para desenvolvimentos internos quanto terceirizados de código;

b) práticas e defeitos de codificação comuns e históricos que levem a vulnerabilidades de segurança da informação;

c) configuração de ferramentas de desenvolvimento, como ambientes integrados de desenvolvimento (IDE), para ajudar a impor a criação de código seguro;

d) orientações emitidas pelos provedores de ferramentas de desenvolvimento e ambientes de execução, conforme aplicável;

e) manutenção e uso de ferramentas de desenvolvimento atualizadas (por exemplo, compiladores);

f) qualificação de desenvolvedores na escrita de código seguro;

g) *design* e arquitetura seguros, incluindo modelagem de ameaças;

h) padrões de codificação seguros e, quando relevante, obrigando seu uso;

i) uso de ambientes controlados para o desenvolvimento.

Durante a codificação

Convém que as considerações durante a codificação incluam:

a) práticas de codificação seguras específicas das linguagens e técnicas de programação que estão sendo utilizadas;

b) utilização de técnicas seguras de programação, como programação em duplas, *refactoring*, revisão por pares, iterações de segurança e desenvolvimento orientado por testes;

c) utilização de técnicas estruturadas de programação;

d) documentação de códigos e remoção de defeitos de programação, que podem permitir a exploração de vulnerabilidades de segurança da informação;

e) proibição do uso de técnicas de *design* inseguras (por exemplo, uso de senhas no código-fonte, amostras de código não aprovadas e serviços *web* não autenticados).

Convém que os testes sejam realizados durante e após o desenvolvimento (ver 8.29). Os processos de teste de segurança de aplicações estáticas (SAST) podem identificar vulnerabilidades de segurança no *software*.

Antes de o *software* ser operacionalizado, convém que o seguinte seja avaliado:

a) superfície de ataque e princípio do menor privilégio;

b) condução de uma análise dos erros de programação mais comuns e documentação de como estes erros foram mitigados.

Análise crítica e manutenção

Após o código ter sido operacionalizado:

a) convém que as atualizações sejam empacotadas e implantadas com segurança;

b) convém que vulnerabilidades de segurança da informação relatadas sejam tratadas (ver 8.8);

c) convém que erros e suspeitas de ataques sejam registrados e que os *logs* sejam analisados criticamente de forma regular, para fazer ajustes no código conforme necessário;

d) convém que o código-fonte seja protegido contra acesso e adulteração não autorizados (por exemplo, usando ferramentas de gerenciamento de configuração, que normalmente fornecem recursos como controle de acesso e controle de versão).

Se forem usadas ferramentas externas e bibliotecas, convém que as organizações considerem:

a) assegurar que as bibliotecas externas sejam gerenciadas (por exemplo, mantendo um inventário de bibliotecas utilizadas e suas versões) e atualizadas regularmente com ciclos de lançamento;

b) selecionar, autorizar e reutilizar componentes bem avaliados, particularmente autenticação e componentes criptográficos;

c) utilizar licença, segurança e histórico dos componentes externos;

d) assegurar que o *software* seja mantido, rastreado e originário de fontes comprovadas e respeitáveis;

e) disponibilizar suficientemente, a longo prazo, recursos de desenvolvimento e artefatos.

Quando um pacote de *software* precisar ser modificado, convém que sejam considerados os seguintes pontos:

a) o risco de controles incorporados e processos de integridade serem comprometidos;

b) obtenção do consentimento do fornecedor;

c) possibilidade de obter as alterações necessárias do fornecedor como atualizações-padrão do programa;

d) impacto se a organização se tornar responsável pela manutenção futura do *software* como resultado de mudanças;

e) compatibilidade com outros *softwares* em uso.

Outras informações

Um princípio norteador é assegurar que o código relevante para a segurança seja invocado quando necessário e seja resistente a adulterações. Os programas instalados a partir do código binário compilado também têm essas propriedades, mas apenas para dados mantidos dentro do aplicativo.

Para linguagens interpretadas, o conceito só funciona quando o código é executado em um servidor que é inacessível pelos usuários e processos que o utilizam, e quando seus dados são mantidos em um banco de dados protegido da mesma forma. Por exemplo, o código interpretado pode ser executado em um serviço de nuvem em que o acesso ao próprio código requeira privilégios de administrador. Convém que esse acesso de administrador seja protegido por mecanismos de segurança, como princípios de administração *just-in-time* e autenticação forte. Se o proprietário da aplicação puder acessar *scripts* por acesso remoto direto ao servidor, então, em princípio, um invasor também pode. Convém que os servidores *web* sejam configurados para evitar a navegação em diretórios, nesses casos.

O código da aplicação é melhor projetado na suposição de que ele está sempre sujeito a ataque por erro ou ação maliciosa. Além disso, aplicações críticas podem ser projetadas para serem tolerantes a falhas internas. Por exemplo, a saída de um algoritmo complexo pode ser verificada para assegurar que ele esteja dentro de limites seguros antes que os dados sejam usados em uma aplicação, como uma aplicação crítica de segurança ou financeira. O código que executa as verificações de limites é simples e, portanto, muito mais fácil de provar que está correto.

Algumas aplicações da *web* são suscetíveis a uma variedade de vulnerabilidades que são introduzidas por *design* e codificação ruins, como injeção em banco de dados e ataques de *scripting* entre *sites*. Nesses ataques, as solicitações podem ser manipuladas para abusar da funcionalidade do servidor *web*.

Mais informações sobre a avaliação de segurança de TIC podem ser encontradas na série ISO/IEC 15408.

8.29 Testes de segurança em desenvolvimento e aceitação

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Identificar	#Segurança_de_aplicação #Garantia_de_segurança_da_informação #Segurança_de_sistemas_e_rede	#Proteção

Controle

Convém que os processos de teste de segurança sejam definidos e implementados no ciclo de vida do desenvolvimento.

Propósito

Validar se os requisitos de segurança da informação são atendidos quando as aplicações ou códigos são implantados no ambiente de produção.

Orientação

Convém que novos sistemas de informação, *upgrades* e novas versões sejam exaustivamente testados e verificados durante os processos de desenvolvimento. Convém que os testes de segurança sejam parte integrante dos testes para sistemas ou seus componentes.

Convém que os testes de segurança sejam realizados com um conjunto de requisitos, que podem ser expressos como funcionais ou não funcionais. Convém que os testes de segurança incluam testes de:

a) funções de segurança [por exemplo, autenticação do usuário (ver 8.5), restrição de acesso (ver 8.3) e uso de criptografia (ver 8.24)];

b) codificação segura (ver 8.28);

c) configurações seguras (ver 8.9, 8.20 e 8.22), incluindo a de sistemas operacionais, *firewalls* e outros componentes de segurança.

Convém que os planos de teste sejam determinados usando um conjunto de critérios. Convém que a extensão dos testes seja proporcional à importância, à natureza do sistema e ao impacto potencial da mudança que está sendo introduzida. Convém que o plano de testes inclua:

a) cronograma detalhado de atividades e testes;

b) entradas e saídas esperadas sob uma série de condições;

c) critérios para avaliar os resultados;

d) decisão para outras ações, conforme necessário.

A organização pode aproveitar ferramentas automatizadas, como ferramentas de análise de código ou *scanners* de vulnerabilidade, e convém que verifique a correção dos defeitos de segurança relacionados.

Para a evolução interna, convém que esses testes sejam realizados inicialmente pela equipe de desenvolvimento. Convém, então, que testes de aceitação independentes sejam realizados para assegurar que o sistema funcione como esperado e apenas como esperado (ver 5.8). Convém que seja considerado o seguinte:

a) realização de atividades de análise crítica de códigos como elemento relevante para testes de falhas de segurança, incluindo insumos e condições não antecipadas;

b) realização de varredura de vulnerabilidades para identificar configurações inseguras e vulnerabilidades do sistema;

c) realização de testes de invasão para identificar código e arquitetura inseguros.

Para componentes terceirizados de desenvolvimento e compras, convém que seja seguido um processo de aquisição. Convém que os contratos com o fornecedor atendam aos requisitos de segurança identificados (ver 5.20). Convém que os produtos e serviços sejam avaliados em relação a esses critérios antes da aquisição.

Convém que os testes sejam realizados em um ambiente de teste que seja o mais similar possível ao ambiente-alvo de produção, para assegurar que o sistema não introduza vulnerabilidades ao ambiente da organização e que os testes sejam confiáveis (ver 8.31).

Outras informações

Podem ser estabelecidos vários ambientes de teste, que podem ser usados para diferentes tipos de testes (por exemplo, testes funcionais e de desempenho). Esses diferentes ambientes podem ser virtuais, com configurações individuais que simulem uma variedade de ambientes operacionais.

Testes e monitoramento de ambientes de teste, ferramentas e tecnologias também precisam ser considerados para assegurar testes eficazes. As mesmas considerações se aplicam ao monitoramento dos sistemas de monitoramento implantados nas configurações de desenvolvimento, teste e produção. É necessário julgar, guiado pela sensibilidade dos sistemas e dados, para determinar quantas camadas de metateste são úteis.

8.30 Desenvolvimento terceirizado

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo #Detectivo	#Confidencialidade #Integridade #Disponibilidade	#Identificar #Detectar #Proteger	#Segurança_de_sistemas_e_rede #Segurança_de_ aplicação #Segurança_nas_relações_com_ fornecedores	#Governança_e_ ecossistema #Proteção

Controle

Convém que a organização dirija, monitore e analise criticamente as atividades relacionadas à terceirização de desenvolvimento de sistemas.

Propósito

Assegurar que as medidas de segurança da informação requeridas pela organização sejam implementadas na terceirização do desenvolvimento de sistemas.

Orientação

Quando o desenvolvimento do sistema é terceirizado, convém que a organização comunique e concorde com requisitos e expectativas, monitore e analise criticamente de forma contínua se a entrega de trabalhos terceirizados atende a essas expectativas. Convém que os seguintes pontos sejam considerados em toda a cadeia de fornecimento externa da organização:

a) contratos de licenciamento, propriedade de código e direitos de propriedade intelectual relacionados com o conteúdo de terceiros (ver 5.32);

b) requisitos contratuais para práticas seguras de projeto, codificação e teste (ver 8.25 a 8.29);

c) provisão do modelo de ameaça a ser considerado por desenvolvedores externos;

d) teste de aceitação para a qualidade e precisão dos produtos (ver 8.29);

e) provisão de evidências de que níveis mínimos aceitáveis de segurança e capacidades de privacidade estão estabelecidos (por exemplo, relatórios de garantia);

f) provisão de evidências de que testes suficientes foram aplicados para proteger contra a presença de conteúdo malicioso (intencional e não intencional) após a entrega;

g) provisão de evidências de que testes suficientes foram aplicados para proteger contra a presença de vulnerabilidades conhecidas;

h) contratos de custódia para o código-fonte do *software* (por exemplo, se o fornecedor sair do negócio);

i) direito contratual para auditar processos e controles de desenvolvimento;

j) requisitos de segurança para o ambiente de desenvolvimento (ver 8.31);

k) consideração da legislação aplicável (por exemplo, sobre proteção de dados pessoais).

Outras informações

Mais informações sobre relacionamentos com fornecedores podem ser encontradas na série ISO/IEC 27036.

8.31 Separação dos ambientes de desenvolvimento, teste e produção

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Segurança_de_aplicação #Segurança_de_sistemas_e_rede	#Proteção

Controle

Convém que ambientes de desenvolvimento, testes e produção sejam separados e protegidos.

Propósito

Proteger o ambiente de produção e os dados de comprometimento por meio de atividades de desenvolvimento e teste.

Orientação

Convém que o nível de separação entre ambientes de produção, testes e desenvolvimento necessários para evitar problemas de produção seja identificado e implementado.

Convém que os seguintes itens sejam considerados:

a) separar adequadamente os sistemas de desenvolvimento e produção e operação deles em diferentes domínios (por exemplo, em ambientes virtuais ou físicos separados);

b) definir, documentar e implementar regras e autorização para a implantação de *software* do desenvolvimento ao *status* de produção;

c) testar alterações nos sistemas de produção e aplicações em um ambiente de teste ou preparação antes de serem aplicados aos sistemas de produção (ver 8.29);

d) não testar em ambientes de produção, exceto em circunstâncias que foram definidas e aprovadas;

e) compiladores, editores e outras ferramentas de desenvolvimento ou programas utilitários não sendo acessíveis a partir de sistemas de produção, quando não necessário;

f) exibir de etiquetas de identificação de ambiente adequadas nos menus para reduzir o risco de erro;

g) não copiar informações sensíveis nos ambientes de desenvolvimento e teste do sistema, a menos que sejam fornecidos controles equivalentes para os sistemas de desenvolvimento e teste.

Em todos os casos, convém que os ambientes de desenvolvimento e teste sejam protegidos considerando:

a) *patches* e atualização de todas as ferramentas de desenvolvimento, integração e teste (incluindo construtores, integradores, compiladores, sistemas de configuração e bibliotecas);

b) configuração segura de sistemas e *software*;

c) controle do acesso aos ambientes;

d) monitoramento da mudança no ambiente e código armazenado nele;

e) monitoramento seguro dos ambientes;

f) *backup* das informações dos ambientes.

Convém que uma única pessoa não tenha a capacidade de fazer alterações tanto no desenvolvimento quanto na produção sem uma análise crítica e aprovação prévias. Isso pode ser alcançado, por exemplo, pela segregação de direitos de acesso ou por regras que são monitoradas. Em situações excepcionais, convém que sejam implementadas medidas adicionais como registro detalhado e monitoramento em tempo real para detectar e agir sobre alterações não autorizadas.

Outras informações

Sem medidas e procedimentos adequados, os desenvolvedores e testadores que tenham acesso a sistemas de produção podem introduzir riscos significativos (por exemplo, modificação indesejada de arquivos ou ambiente do sistema, falha no sistema, execução de código não autorizado e não testado em sistemas de produção, divulgação de dados confidenciais, problemas de integridade e disponibilidade de dados). É necessário manter um ambiente conhecido e estável para realizar testes significativos e impedir o acesso inadequado do desenvolvedor ao ambiente de produção.

As medidas e procedimentos incluem papéis cuidadosamente projetados em conjunto com a implementação de requisitos de segregação de funções e possuem processos de monitoramento adequados em vigor.

O pessoal de desenvolvimento e testes também representa uma ameaça à confidencialidade das informações de produção. Atividades de desenvolvimento e teste podem causar alterações não intencionais no *software* ou informações, se compartilharem o mesmo ambiente computacional. A separação de ambientes de desenvolvimento, testes e produção é, portanto, desejável para reduzir o risco de alteração acidental ou acesso não autorizado a *softwares* de produção e dados de negócios (ver 8.33 para a proteção de informações de teste).

Em alguns casos, a distinção entre ambientes de desenvolvimento, teste e produção pode ser deliberadamente acobertada, e os testes podem ser realizados em um ambiente de desenvolvimento ou por meio de planos de implantação controlados para usuários ou servidores ativos (por exemplo, pequena população de usuários-piloto). Em alguns casos, os testes de produtos podem ocorrer pelo uso ao vivo do produto dentro da organização. Além disso, para reduzir o tempo de inatividade das implantações ao vivo, dois ambientes de produção idênticos podem ser apoiados, em que apenas um está ao vivo ao mesmo tempo.

Processos de suporte para o uso de dados de produção em ambientes de desenvolvimento e teste (8.33) são necessários.

As organizações também podem considerar as orientações fornecidas nesta Seção para ambientes de treinamento, ao realizar o treinamento do usuário final.

8.32 Gestão de mudanças

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Segurança_de_aplicação #Segurança_de_sistemas_e_rede	#Proteção

Controle

Convém que mudanças nos recursos de tratamento de informações e sistemas de informação estejam sujeitas a procedimentos de gestão de mudanças.

Propósito

Preservar a segurança da informação ao executar mudanças.

Orientação

Convém que a introdução de novos sistemas e grandes mudanças nos sistemas existentes sigam as regras acordadas e um processo formal de documentação, especificação, testes, controle de qualidade e implementação gerenciada. Convém que as responsabilidades e os procedimentos de gestão estejam em vigor para assegurar o controle satisfatório de todas as mudanças.

Convém que os procedimentos de controle de mudanças sejam documentados e aplicados para assegurar a confidencialidade, integridade e disponibilidade de informações em recursos de tratamento de informações e sistemas de informação, para todo o ciclo de vida de desenvolvimento do sistema, desde os estágios iniciais de projeto até todos os esforços subsequentes de manutenção.

Convém que, sempre que possível, os procedimentos de controle de alteração para infraestrutura e *software* de TIC sejam integrados.

Convém que os procedimentos de controle de alteração incluam:

a) planejamento e avaliação do impacto potencial das mudanças, considerando todas as dependências;

b) autorização de mudanças;

c) comunicação de mudanças às partes interessadas pertinentes;

d) testes e aceitação de testes para as mudanças (ver 8.29);

e) implementação de mudanças, incluindo planos de implantação;

f) considerações de emergência e contingência, incluindo procedimentos de retorno;

g) manutenção de registros de mudanças que incluam todos os itens acima;

h) garantia de que a documentação operacional (ver 5.37) e os procedimentos do usuário sejam alterados conforme necessário para permanecer apropriados;

i) garantia de que os planos de continuidade das TIC e os procedimentos de resposta e recuperação (ver 5.30) sejam alterados conforme necessário para que permaneçam apropriados.

Outras informações

O controle inadequado das mudanças nos recursos de tratamento de informações e sistemas de informação é uma causa comum de falhas de sistema ou segurança. Mudanças no ambiente de produção, especialmente ao transferir *softwares* do desenvolvimento para o ambiente operacional, podem impactar na integridade e disponibilidade de aplicações.

A mudança de *software* pode impactar o ambiente de produção e vice-versa.

A boa prática inclui o teste de componentes de TIC em um ambiente segregado de ambos os ambientes de produção e desenvolvimento (veja 8.31). Isto provê um meio de ter controle sobre um novo *software* e permitir proteção adicional de informações operacionais que são usadas para fins de teste. Convém que isso inclua *patches*, pacotes de serviço e outras atualizações.

O ambiente de produção inclui sistemas operacionais, bancos de dados e plataformas de *middleware*. Convém que o controle seja aplicado para mudanças de aplicações e infraestruturas.

8.33 Informações de teste

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade	#Proteger	#Proteção_da_informação	#Proteção

Controle

Convém que as informações de teste sejam adequadamente selecionadas, protegidas e gerenciadas.

Propósito

Assegurar a relevância dos testes e a proteção das informações operacionais utilizadas para testes.

Orientação

Convém que as informações de teste sejam selecionadas para assegurar a confiabilidade dos resultados dos testes e a confidencialidade das informações operacionais relevantes. Convém que as informações sensíveis (incluindo dados pessoais) não sejam copiadas para os ambientes de desenvolvimento e teste (ver 8.31).

Convém que as seguintes diretrizes sejam aplicadas para proteger as cópias das informações operacionais, quando usadas para fins de teste, quer o ambiente de teste seja construído internamente ou em um serviço em nuvem:

a) aplicar os mesmos procedimentos de controle de acesso para testar ambientes como os aplicados aos ambientes operacionais;

b) ter uma autorização separada cada vez que as informações operacionais forem copiadas para um ambiente de teste;

c) registrar a cópia e o uso de informações operacionais para fornecer uma trilha de auditoria;

d) proteger informações sensíveis por remoção ou mascaramento (ver 8.11), se usadas para testes;

e) excluir corretamente (ver 8.10) as informações operacionais de um ambiente de teste imediatamente após os testes estarem completos, para evitar o uso não autorizado de informações de teste.

Convém que as informações de teste sejam armazenadas com segurança (para evitar adulteração, o que pode levar a resultados inválidos) e usadas apenas para fins de teste.

Outras informações

Testes de sistema e aceitação podem requerer volumes substanciais de informações de teste que são tão próximos quanto possível das informações operacionais.

8.34 Proteção de sistemas de informação durante os testes de auditoria

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Segurança_de_sistemas_e_rede #Proteção_da_informação	#Governança_e_ecossistema #Proteção

Controle

Convém que testes de auditoria e outras atividades de garantia envolvendo a avaliação de sistemas operacionais sejam planejados e acordados entre o testador e a gestão apropriada.

Propósito

Minimizar o impacto da auditoria e outras atividades de garantia em sistemas operacionais e processos de negócio.

Orientação

Convém que sejam observadas as seguintes diretrizes:

a) acordar pedidos de acesso da auditoria a sistemas e dados com a gestão apropriada;

b) acordar e controlar o escopo dos testes de auditoria técnica;

c) limitar testes de auditoria a acesso somente para leitura de *software* e dados. Se o acesso somente para leitura não estiver disponível para obter as informações necessárias, executar o teste por um administrador experiente que tenha os direitos de acesso necessários em nome do auditor;

d) se o acesso for concedido, estabelecer e verificar os requisitos de segurança (por exemplo, antivírus e *patches*) dos dispositivos utilizados para acessar os sistemas (por exemplo, *laptops* ou *tablets*) antes de permitir o acesso;

e) permitir acesso além de somente leitura apenas para cópias isoladas de arquivos do sistema, excluí-las quando a auditoria for concluída ou fornecer proteção adequada, se houver a obrigação de manter tais arquivos de acordo com os requisitos de documentação de auditoria;

f) identificar e concordar com os pedidos de tratamento especial ou adicional, como a execução de ferramentas de auditoria;

g) executar testes de auditoria que podem afetar a disponibilidade do sistema fora do horário comercial;

h) monitorar e registrar todo o acesso para fins de auditoria e teste.

Outras informações

Testes de auditoria e outras atividades de garantia também podem acontecer em sistemas de desenvolvimento e teste, em que tais testes podem impactar, por exemplo, a integridade do código ou levar à divulgação de quaisquer informações sensíveis mantidas em tais ambientes.

Anexo A
(informativo)

Uso de atributos

A.1 Geral

Este Anexo fornece uma tabela para demonstrar o uso de atributos como forma de criar diferentes visões dos controles. Os cinco exemplos desses atributos são os seguintes (ver 4.2):

a) Tipos de controle (#Preventivo, #Detectivo, #Corretivo)

b) Propriedades de segurança da informação (#Confidencialidade, #Integridade, #Disponibilidade)

c) Conceitos de segurança cibernética (#Identificar, #Proteger, #Detectar, #Responder, #Restaurar)

d) Capacidades operacionais (#Governança, #Gestão_de_ativos #Proteção_da_informação, #Segurança_em_recursos_humanos, #Segurança_física, #Segurança_de_sistemas_e_rede, #Segurança_de_aplicação, #Configuração_segura, #Gestão_de_identidade_e_acesso,#Gestão_de_ameaças_e_vulnerabilidades, #Continuidade, #Segurança_nas_relações_com_fornecedores, #Leis_e_*compliance*, #Gestão_de_eventos_de_segurança_da_informação, #Garantia_de_segurança_da_informação)

e) Domínios de segurança (#Governança_e_ecossistema, #Proteção, #Defesa, #Resiliência)

A Tabela A.1 contém uma matriz de todos os controles neste documento, com seus valores de atributos dados.

A filtragem ou classificação da matriz pode ser alcançada usando uma ferramenta como uma planilha simples ou um banco de dados, que pode incluir mais informações, como texto de controle, orientação, orientação específica da organização ou atributos (ver A.2).

Tabela A.1 – Matriz de controles e valores de atributos (continua)

ABNT NBR ISO/IEC 27002 Identificador do controle	Nome do controle	Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
5.1	Políticas de segurança da informação	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Identificar	#Governança	#Governança_e_ecossistema #Resiliência
5.2	Funções e responsabilidades de segurança da informação	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Identificar	#Governança	#Governança_e_ecossistema #Proteção #Resiliência

Tabela A.1 (continuação)

ABNT NBR ISO/IEC 27002 Identificador do controle	Nome do controle	Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
5.3	Segregação de funções	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Governança #Gestão_de_ identidade_e_acesso	# Governança_e_ ecossistema
5.4	Responsabilidades da direção	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Identificar	#Governança	# Governança_e_ ecossistema
5.5	Contato com autoridades	#Preventivo #Corretivo	#Confidencialidade #Integridade #Disponibilidade	#Identificar #Proteger #Responder #Restaurar	#Governança	#Defesa #Resiliência
5.6	Contato com grupos de interesses especial	#Preventivo #Corretivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger #Responder #Restaurar	#Governança	#Defesa
5.7	Inteligência de ameaças	#Preventivo #Detectivo #Corretivo	#Confidencialidade #Integridade #Disponibilidade	#Identificar #Detectar #Responder	#Gestão_de_ ameaças_e_ vulnerabilidades	#Defesa #Resiliência
5.8	Segurança da informação no gerenciamento de projeto	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Identificar #Proteger	#Governança	# Governança_e_ ecossistema #Proteção
5.9	Inventário de informações e outros ativos associados	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Identificar	#Gestão_de_ativos	# Governança_e_ ecossistema #Proteção
5.10	Uso aceitável de informações e outros ativos associados	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Gestão_de_ativos #Proteção_da_ informção	# Governança_e_ ecossistema #Proteção
5.11	Devolução de ativos	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Gestão_de_ativos	#Proteção
5.12	Classificação das informações	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Identificar	#Proteção_da_ informação	#Proteção #Defesa
5.13	Rotulagem de informações	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Proteção_da_ informação	#Defesa #Proteção

Tabela A.1 (continuação)

ABNT NBR ISO/IEC 27002 Identificador do controle	Nome do controle	Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
5.14	Transferência de informações	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Gestão_de_ativos #Proteção_da_ informação	#Proteção
5.15	Controle de acesso	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Gestão_de_ identidade_e_acesso	#Proteção
5.16	Gestão de identidade	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Gestão_de_ identidade_e_acesso	#Proteção
5.17	Informações de autenticação	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Gestão_de_ identidade_e_acesso	#Proteção
5.18	Direitos de acesso	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Gestão_de_ identidade_e_acesso	#Proteção
5.19	Segurança da informação nas relações com fornecedores	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Identificar	#Segurança_nas_ relações_com_ fornecedores	# Governança_e_ Ecossistema #Proteção
5.20	Abordagem da segurança da informação nos contratos de fornecedores	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Identificar	#Segurança_nas_ relações_com_ fornecedores	# Governança_e_ ecossistema #Proteção
5.21	Gestão da segurança da informação na cadeia de fornecimento de TIC	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Identificar	#Segurança_nas_ relações_com_ fornecedores	# Governança_e_ ecossistema #Proteção
5.22	Monitoramento, análise crítica e gestão de mudanças dos serviços de fornecedores	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Identificar	#Segurança_nas_ relações_com_ fornecedores	# Governança_e_ ecossistema #Proteção #Defesa #Garantia_de_ segurança_da_ informação

Tabela A.1 (continuação)

ABNT NBR ISO/IEC 27002 Identificador do controle	Nome do controle	Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
5.23	Segurança da informação para uso de serviços em nuvem	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Segurança_nas_relações_com_fornecedores	# Governança_e_Ecossistema #Proteção
5.24	Planejamento e preparação da gestão de incidentes de segurança da informação	#Corretivo	#Confidencialidade #Integridade #Disponibilidade	#Responder #Restaurar	#Governança #Gestão_de_evento_de_segurança_da_informação	#Defesa
5.25	Avaliação e decisão sobre eventos de segurança de informação	#Detectivo	#Confidencialidade #Integridade #Disponibilidade	#Detectar #Responder	#Gestão_de_evento_de_segurança_da_informação	#Defesa
5.26	Resposta a incidentes de segurança da informação	#Corretivo	#Confidencialidade #Integridade #Disponibilidade	#Responder #Restaurar	#Gestão_de_evento_de_segurança_da_informação	#Defesa
5.27	Aprendizado com incidentes de segurança da informação	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Identificar #Proteger	#Gestão_de_evento_de_segurança_da_informação	#Defesa
5.28	Coleta de evidências	#Corretivo	#Confidencialidade #Integridade #Disponibilidade	#Detectar #Responder	#Gestão_de_evento_de_segurança_da_informação	#Defesa
5.29	Segurança da informação durante a disrupção	#Preventivo #Corretivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger #Responder	#Continuidade	#Resiliência #Proteção
5.30	Prontidão de TIC para continuidade de negócios	#Corretivo	#Disponibilidade	#Responder	#Continuidade	#Resiliência
5.31	Requisitos legais, estatutários, regulamentares e contratuais	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Identificar	#Leis_e_*compliance*	#Governança_e_ecossistema #Proteção
5.32	Direitos de propriedade intelectual	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Identificar	#Leis_e_compliance	#Governança_e_ecossistema

Tabela A.1 (continuação)

ABNT NBR ISO/IEC 27002 Identificador do controle	Nome do controle	Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
5.33	Proteção de registros	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Identificar #Proteger	#Leis_e_compliance #Gestão_de_ativos #Proteção_da_ informação	#Defesa
5.34	Privacidade e proteção de DP	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Identificar #Proteger	#Proteção_da_ informação #Leis_e_compliance	#Proteção
5.35	Análise crítica independente da segurança da informação	#Preventivo #Corretivo	#Confidencialidade #Integridade #Dispon bilidade	#Identificar #Proteger	#Garantia_de_ segurança_da_ informação	#Governança_e_ ecossistema
5.36	Conformidade com políticas, regras e normas de segurança da informação	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Identificar #Proteger	#Leis_e_compliance #Garantia_de_ segurança_ da_ informação	#Governança_e_ ecossistema
5.37	Documentação dos procedimentos de operação	#Preventivo #Corretivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger #Restaurar	#Gestão_de_ativos #Segurança_física #Segurança_de_ _sistemas_e_rede #Segurança_ de_aplicações #Configuração_ segura #Gestão_de_ identidade_e_acesso #Gestão_de_ ameaças_e_ vulnerabilidades #Continuidade #Gestão_de_ eventos_de_ segurança_da_ informação	#Governança_e_ ecossistema #Proteção #Defesa
6.1	Seleção	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Segurança_em_ recursos_humanos	#Governança_e_ ecossistema
6.2	Termos e condições de contratação	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Segurança_em_ recursos_humanos	#Governança_e_ ecossistema

Tabela A.1 (continuação)

ABNT NBR ISO/IEC 27002 Identificador do controle	Nome do controle	Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
6.3	Conscientização, educação e treinamento em segurança da informação	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Segurança_em_ recursos_humanos	#Governança_e_ ecossistemaem
6.4	Processo disciplinar	#Preventivo #Corretivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger #Responder	#Segurança_em_ recursos_humanos	#Governança_e_ ecossistema
6.5	Responsabilidades após encerramento ou mudança da contratação	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Segurança_em_ recursos_humanos #Gestão_de_ativos	#Governança_e_ ecossistema
6.6	Acordos de confidencialidade ou não divulgação	#Preventivo	#Confidencialidade	#Proteger	#Segurança_em_ recursos_humanos #Proteção_da_ informação #Segurança_nas_ relações_com_ fornecedores	#Governança_e_ ecossistema
6.7	Trabalho remoto	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Gestão_de_ativos #Proteção_ da_informação #Segurança_física #Segurança_de_ sistemas_e_rede	#Proteção
6.8	Relatos de eventos de segurança da informação	#Detectivo	#Confidencialidade #Integridade #Disponibilidade	#Detectar	#Gestão_de_ eventos_de_ segurança_da_ informação	#Defesa
7.1	Perímetros de segurança física	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Segurança_física	#Proteção
7.2	Entrada física	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Segurança_física #Gestão_de_ identidades_e_ acesso	#Proteção
7.3	Segurança de escritórios, salas e instalações	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Segurança_física #Gestão_de_ativos	#Proteção

Tabela A.1 (continuação)

ABNT NBR ISO/IEC 27002 Identificador do controle	Nome do controle	Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
7.4	Monitoramento de segurança física	#Preventivo #Detectivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger #Detectar	#Segurança_física	#Proteção #Defesa
7.5	Proteção contra ameaças físicas e ambientais	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Segurança_física	#Proteção
7.6	Trabalho em áreas seguras	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Segurança_física	#Proteção
7.7	Mesa limpa e tela limpa	#Preventivo	#Confidencialidade	#Proteger	#Segurança_física	#Proteção
7.8	Localização e proteção do equipamento	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Segurança_física #Gestão_de_ativos	#Proteção
7.9	Segurança de ativos fora das dependências da organização	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Segurança_física #Gestão_de_ativos	#Proteção
7.10	Mídia de armazenamento	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Segurança_física #Gestão_de_ativos	#Proteção
7.11	Serviços de infraestrutura	#Preventivo #Detectivo	#Integridade #Disponibilidade	#Proteger #Detectar	#Segurança_física	#Proteção
7.12	Segurança do cabeamento	#Preventivo	#Confidencialidade #Disponibilidade	#Proteger	#Segurança_física	#Proteção
7.13	Manutenção de equipamentos	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	# Segurança_física #Gestão_de_ativos	#Proteção #Resiliência
7.14	Descarte seguro ou reutilização de equipamentoss	#Preventivo	#Confidencialidade	#Proteger	# Segurança_física #Gestão_de_ativos	#Proteção
8.1	Dispositivos *endpoint* do usuário	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Gestão_de_ativos #Proteção_da_ informação	#Proteção
8.2	Direitos de acessos privilegiados	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	# Gestão_de_ identidade_e_acesso	#Proteção

Tabela A.1 (continuação)

ABNT NBR ISO/IEC 27002 Identificador do controle	Nome do controle	Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
8.3	Restrição de acesso à informação	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	# Gestão_de_ identidade_e_acesso	#Proteção
8.4	Acesso ao código-fonte	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	# Gestão_de_ identidade_e_acesso #Segurança_ de_aplicações #Configuração_de_ segurança	#Proteção
8.5	Autenticação segura	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Gestão_de_ identidade_e_acesso	#Proteção
8.6	Gestão de capacidade	#Preventivo #Detectivo	#Integridade #Disponibilidade	#Identificar #Proteger #Detectar	#Continuidade	#Governança_e_ ecossistema #Proteção
8.7	Proteção contra *malware*	#Preventivo #Detectivo #Corretivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger #Detectar	#Segurança_de__ sistemas_e_rede #Proteção_da_ informação	#Proteção #Defesa
8.8	Gestão de vulnerabilidades técnicas	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Identificar #Proteger	#Gestão_de_ ameaças_e_ vulnerabilidades	#Governança_e_ ecossistema #Proteção #Defesa
8.9	Gestão de configuração	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Configuração_ segura	#Proteção
8.10	Exclusão de informações	#Preventivo	#Confidencialidade	#Proteger	#Proteção_da_ informação #Legal_e_ compliance	#Proteção
8.11	Mascaramento de dados	#Preventivo	#Confidencialidade	#Proteger	#Proteção_da_ informação	#Proteção
8.12	Prevenção de vazamento de dados	#Preventivo #Detectivo	#Confidencialidade	#Proteger #Detectar	#Proteção_da_ informação	#Proteção #Defesa
8.13	*Backup* das Informações	#Corretivo	#Integridade #Disponibilidade	#Restaurar	#Continuidade	#Proteção

Tabela A.1 (continuação)

ABNT NBR ISO/IEC 27002 Identificador do controle	Nome do controle	Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
8.14	Redundância dos recursos de tratamento de informações	#Preventivo	#Disponibilidade	#Proteger	#Continuidade #Gestão_de_ativos	#Proteção #Resiliência
8.15	*Log*	#Detectivo	#Confidencialidade #Integridade #Disponibilidade	#Detectar	#Gestão_de_ eventos_de_ segurança_da_ informação	#Proteção #Defesa
8.16	Atividades de monitoramento	#Detectivo #Corretivo	#Confidencialidade #Integridade #Disponibilidade	#Detectar #Responder	#Gestão_de_ eventos_de_ segurança_da_ informação	#Proteção
8.17	Sincronização do relógio	#Detectivo	#Integridade	#Proteger #Detectar	#Gestão_de_ eventos_de_ segurança_da_ informação	#Proteção #Defesa
8.18	Uso de programas utilitários privilegiados	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Segurança_de_ _sistemas_e_rede #Configuração_ segura #Segurança_de_ aplicações	#Proteção
8.19	Instalação de *software* em sistemas operacionais	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Configuração_de_ segura#Segurança_ de_aplicações	#Proteção
8.20	Segurança de redes	#Preventivo #Detectivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger #Detectar	#Segurança_de_ _sistemas_e_rede	#Proteção
8.21	Segurança dos serviços de rede	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Segurança_de_ _sistemas_e_rede	#Proteção
8.22	Segregação de redes	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Segurança_de_ _sistemas_e_rede	#Proteção
8.23	Filtragem da *web*	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Segurança_de__ sistemas_e_rede	#Proteção

Tabela A.1 (continuação)

ABNT NBR ISO/IEC 27002 Identificador do controle	Nome do controle	Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
8.24	Uso de criptografia	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Configuração_de_segura	#Proteção
8.25	Ciclo de vida de desenvolvimento seguro	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Segurança_de_aplicações #Segurança_de_sistemas_e_rede	#Proteção
8.26	Requisitos de segurança da aplicação	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Segurança_de_aplicações #Segurança_de_sistemas_e_rede	#Proteção #Defesa
8.27	Princípios de arquitetura e engenharia de sistemas seguros	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Segurança_de_aplicações #Segurança_de_sistemas_e_rede	#Proteção
8.28	Codificação segura	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Segurança_de_aplicações #Segurança_de_sistemas_e_rede	#Proteção
8.29	Testes de segurança em desenvolvimento e aceitação	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Identificar	#Segurança_de_aplicações #Garantia_da_segurança_da_informação #Segurança_de_sistemas_e_rede	#Proteção
8.30	Desenvolvimento terceirizado	#Preventivo #Detectivo	#Confidencialidade #Integridade #Disponibilidade	#Identificar #Proteger #Detectar	#Segurança_de_aplicações #Segurança_de_sistemas_e_rede #Segurança_nas_relações_com_fornecedores	#Governança_e_ecossistema #Proteção
8.31	Separação dos ambientes de desenvolvimento, teste e de produção	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Segurança_de_sistemas_e_rede #Segurança_de_aplicações	#Proteção
8.32	Gestão de mudanças	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Segurança_de_sistemas_e_rede #Segurança_de_aplicações	#Proteção

Tabela A.1 (conclusão)

ABNT NBR ISO/IEC 27002 Identificador do controle	Nome do controle	Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
8.33	Informações de testes	#Preventivo	#Confidencialidade #Integridade	#Proteger	#Proteção_da_ informação	#Proteção
8.34	Proteção de sistemas de informação durante testes de auditoria	#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger	#Segurança_de_ sistemas_e_rede #Proteção_da_ informação	#Governança_e_ ecossistema #Proteção

A Tabela A.2 mostra um exemplo de como criar uma exibição, filtrando por um determinado valor de atributo, neste caso #Corretivo.

Tabela A.2 – Visão de controles #Corretivo (continua)

ABNT NBR ISO/IEC 27002 Identificador dos controles	Nome do controle	Tipo do controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidade operacional	Domínio de segurança
5.5	Contato com autoridades	#Preventivo #Corretivo	#Confidencialidade #Integridade #Disponibilidade	#Identificar #Proteger #Responder #Recuperar	#Governança	#Defesa #Resiliência
5.6	Contato com grupos de interesse especial	#Preventivo #Corretivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger #Responder #Recuperar	#Governança	#Defesa
5.7	Inteligência de ameaças	#Preventivo #Detectivo #Corretivo	#Confidencialidade #Integridade #Disponibilidade	#Identificar #Detectar #Responder	#Gestão_de_ ameaças_e_ vulnerabilidades	#Defesa #Resiliência
5.24	Planejamento e preparação da gestão de incidentes de segurança da informação	#Corretivo	#Confidencialidade #Integridade #Disponibilidade	#Responder #Recuperar	#Governança #Gestão_de_ eventos_de_ segurança_da_ informação	#Defesa
5.26	Resposta a incidentes de segurança da informação	#Corretivo	#Confidencialidade #Integridade #Disponibilidade	#Responder #Recuperar	#Gestão_de_ eventos_de_ segurança_da_ informação	#Defesa
5.28	Coleta de evidências	#Corretivo	#Confidencialidade #Integridade #Disponibilidade	#Detectar #Responder	#Gestão_de_ eventos_de_ segurança_da_ informação	#Defesa

Tabela A.2 (conclusão)

ABNT NBR ISO/IEC 27002 Identificador do controle	Nome do controle	Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
5.29	Segurança da informação durante a disrupção	#Preventivo #Corretivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger #Responder	#Continuidade	#Proteção #Resiliência
5.30	Prontidão de TIC para continuidade de negócios	#Corretivo	#Disponibilidade	#Responder	#Continuidade	#Resiliência
5.35	Análise crítica independente da segurança da informação	#Preventivo #Corretivo	#Confidencialidade #Integridade #Disponibilidade	#Identificar #Proteger	#Garantia_da_ segurança_ da_ informação	#Governança_e_ ecossistema
5.37	Procedimentos operacionais documentados	#Preventivo #Corretivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger #Recuperar	#Gestão_de_ativos #Segurança_física #Segurança_de_ sistemas_e_rede #Segurança_de_ aplicações #Configurações de Segurança #Gestão de identidade e de acessos #Gestão de ameaças e de vulnerabilidade #Continuidade #Segurança da Informação – gestão de eventos	#Governança_e_ ecossistema #Proteção #Defesa
6.4	Processo disciplinar	#Preventivo #Corretivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger #Responder	#Segurança em recursos humanos	#Governança_e_ ecossistema
8.7	Proteção contra *malware*	#Preventivo #Detectivo #Corretivo	#Confidencialidade #Integridade #Disponibilidade	#Proteger #Detectar	#Segurança_de_ sistemas_ e_ rede #Proteção_da_ informação	#Proteção #Defesa
8.13	*Backup das* informações	#Corretivo	#Integridade #Disponibilidade	#Recuperar	#Continuidade	#Proteção
8.16	Atividades de monitoramento	#Detectivo #Corretivo	#Confidencialidade #Integridade #Disponibilidade	#Detectar #Responder	#Gestão_de_ eventos_de_ segurança_da_ informação	#Defesa

A.2 Visões organizacionais

Uma vez que atributos são usados para criar diferentes visões dos controles, as organizações podem descartar os exemplos de atributos propostos neste documento e criar seus próprios atributos, com diferentes valores para atender às necessidades específicas da organização. Adicionalmente, os valores designados para cada atributo podem diferir entre organizações, já que organizações podem ter diferentes visões do uso ou aplicabilidade do controle ou dos valores associados ao atributo (quando os valores são específicos ao contexto da organização). O primeiro passo é entender por que um atributo específico da organização é desejável. Por exemplo, se uma organização construiu seus planos de tratamento de risco [ver a ABNT NBR ISO/IEC 27001:2013, 6.1.3 e)] com base em eventos, ela pode desejar associar um atributo de cenário de risco a cada controle neste documento.

O benefício desse atributo é acelerar o processo de cumprimento dos requisitos da ABNT NBR ISO/IEC 27001, relacionados ao tratamento de risco, comparando os controles determinados por meio do processo de tratamento de risco (denominado controles “necessários”), com os da ABNT NBR ISO/IEC 27001:2013, Anexo A (que são abordados neste documento), para assegurar que nenhum controle necessário tenha sido negligenciado.

Uma vez que o propósito e os benefícios são conhecidos, o próximo passo é determinar os valores de atributo. Por exemplo, a organização pode identificar nove eventos:

1) perda ou roubo de dispositivo móvel;
2) perda ou roubo dos recursos da organização;
3) força majoritária, vandalismo e terrorismo;
4) falha de *software*, *hardware*, energia, *internet* e comunicações;
5) fraude;
6) *hacking*;
7) divulgação;
8) violação da lei;
9) engenharia social.

A segunda etapa pode, portanto, ser realizada atribuindo identificadores a cada evento (por exemplo, E1, E2,..., E9).

O terceiro passo é copiar os identificadores de controle e controlar os nomes deste documento em uma planilha ou banco de dados, e associar os valores de atributo a cada controle, lembrando que cada controle pode ter mais de um valor de atributo.

O passo final é classificar a planilha ou consultar o banco de dados para extrair as informações necessárias. Outros exemplos de atributos organizacionais (e possíveis valores) incluem:

a) maturidade (valores da série ISO/IEC 33000 ou outros modelos de maturidade);
b) estado de implementação (a ser implementado, em andamento, parcialmente implementado, totalmente implementado);

c) prioridade (1, 2, 3 etc.);

d) áreas organizacionais envolvidas (segurança, TIC, recursos humanos, Alta Direção etc.);

e) eventos;

f) ativos envolvidos;

g) construção e execução, para diferenciar controles utilizados nas diferentes etapas do ciclo de vida útil;

h) outras metodologias com as quais a organização trabalha ou pode estar em transição para.

Anexo B
(informativo)

Correspondência com a ABNT NBR ISO/IEC 27002:2013

O objetivo deste Anexo é fornecer compatibilidade inversa com a ABNT NBR ISO/IEC 27002:2013 para organizações que atualmente a utilizam e agora desejam fazer a transição para esta edição.

A Tabela B.1 fornece a correspondência dos controles especificados nas Seções 5 a 8 com os da ABNT NBR ISO/IEC 27002:2013.

Tabela B.1 – Correspondência entre os controles deste documento e os controles da ABNT NBR ISO/IEC 27002:2013 (continua)

ABNT NBR ISO/IEC 27002 Identificador do controle	ABNT NBR ISO/IEC 27002:2013 Identificador do controle	Nome do controle
5.1	05.1.1, 05.1.2	Políticas de segurança da informação
5.2	06.1.1	Papéis e responsabilidades pela segurança da informação
5.3	06.1.2	Segregação de funções
5.4	07.2.1	Responsabilidades da direção
5.5	06.1.3	Contato com autoridades
5.6	06.1.4	Contato com grupos de interesse especial
5.7	Novo	Inteligência de ameaças
5.8	06.1.5, 14.1.1	Segurança da informação no gerenciamento de projetos
5.9	08.1.1, 08.1.2	Inventário de informações e outros ativos associados
5.10	08.1.3, 08.2.3	Uso aceitável de informações e outros ativos associados
5.11	08.1.4	Devolução de ativos
5.12	08.2.1	Classificação das informações
5.13	08.2.2	Rotulagem de informações
5.14	13.2.1, 13.2.2, 13.2.3	Transferência de informações
5.15	09.1.1, 09.1.2	Controle de acesso
5.16	09.2.1	Gestão de identidade
5.17	09.2.4, 09.3.1, 09.4.3	Informações de autenticação
5.18	09.2.2, 09.2.5, 09.2.6	Direitos de acesso
5.19	15.1.1	Segurança da informação nas relações com fornecedores

Tabela B.1 (continuação)

ABNT NBR ISO/IEC 27002 Identificador do controle	ABNT NBR ISO/IEC 27002:2013 Identificador do controle	Nome do controle
5.20	15.1.2	Abordagem da segurança da informação nos contratos de fornecedores
5.21	15.1.3	Gestão da segurança da informação na cadeia de fornecimento de TIC
5.22	15.2.1, 15.2.2	Monitoramento, análise crítica e gestão de mudanças dos serviços de fornecedores
5.23	Novo	Segurança da informação para uso de serviços em nuvem
5.24	16.1.1	Planejamento e preparação da gestão de incidentes de segurança da informação
5.25	16.1.4	Avaliação e decisão sobre eventos de segurança da informação
5.26	16.1.5	Resposta a incidentes de segurança da informação
5.27	16.1.6	Aprendizado com incidentes de segurança da informação
5.28	16.1.7	Coleta de evidências
5.29	17.1.1, 17.1.2, 17.1.3	Segurança da informação durante a disrupção
5.30	Novo	Prontidão de TIC para continuidade de negócios
5.31	18.1.1, 18.1.5	Requisitos legais, estatutários, regulamentares e contratuais
5.32	18.1.2	Direitos de propriedade intelectual
5.33	18.1.3	Proteção de registros
5.34	18.1.4	Privacidade e proteção de DP
5.35	18.2.1	Análise crítica independente da segurança da informação
5.36	18.2.2, 18.2.3	Conformidade com políticas, regras e normas para segurança da informação
5.37	12.1.1	Documentação dos procedimentos de operação
6.1	07.1.1	Seleção
6.2	07.1.2	Termos e condições de contratação
6.3	07.2.2	Conscientização, educação e treinamento em segurança da informação
6.4	07.2.3	Processo disciplinar
6.5	07.3.1	Responsabilidades após encerramento ou mudança da contratação

Tabela B.1 (continuação)

ABNT NBR ISO/IEC 27002 Identificador do controle	ABNT NBR ISO/IEC 27002:2013 Identificador do controle	Nome do controle
6.6	13.2.4	Acordos de confidencialidade ou não divulgação
6.7	06.2.2	Trabalho remoto
6.8	16.1.2, 16.1.3	Relato de eventos de segurança da informação
7.1	11.1.1	Perímetros de segurança física
7.2	11.1.2, 11.1.6	Entrada física
7.3	11.1.3	Segurança de escritórios, salas e instalações
7.4	Novo	Monitoramento de segurança física
7.5	11.1.4	Proteção contra ameaças físicas e ambientais
7.6	11.1.5	Trabalho em áreas seguras
7.7	11.2.9	Mesa limpa e tela limpa
7.8	11.2.1	Localização e proteção de equipamentos
7.9	11.2.6	Segurança de ativos fora das instalações da organização
7.10	08.3.1, 08.3.2, 08.3.3, 11.2.5	Mídia de armazenamento
7.11	11.2.2	Serviços de infraestrutura
7.12	11.2.3	Segurança do cabeamento
7.13	11.2.4	Manutenção de equipamentos
7.14	11.2.7	Descarte seguro ou reutilização de equipamentos
8.1	06.2.1, 11.2.8	Dispositivos *endpoint* do usuário
8.2	09.2.3	Direitos de acessos privilegiados
8.3	09.4.1	Restrição de acesso à informação
8.4	09.4.5	Acesso ao código-fonte
8.5	09.4.2	Autenticação segura
8.6	12.1.3	Gestão de capacidade
8.7	12.2.1	Proteção contra *malware*
8.8	12.6.1, 18.2.3	Gestão de vulnerabilidades técnicas
8.9	Novo	Gestão de configuração
8.10	Novo	Exclusão de informações
8.11	Novo	Mascaramento de dados
8.12	Novo	Prevenção de vazamento de dados
8.13	12.3.1	*Backup* das informações
8.14	17.2.1	Redundância dos recursos de tratamento de informações

Tabela B.1 (conclusão)

ABNT NBR ISO/IEC 27002 Identificador do controle	ABNT NBR ISO/IEC 27002:2013 Identificador do controle	Nome do controle
8.15	12.4.1, 12.4.2, 12.4.3	*Log*
8.16	Novo	Atividades de monitoramento
8.17	12.4.4	Sincronização do relógio
8.18	09.4.4	Uso de programas utilitários privilegiados
8.19	12.5.1, 12.6.2	Instalação de *software* em sistemas operacionais
8.20	13.1.1	Segurança de redes
8.21	13.1.2	Segurança dos serviços de rede
8.22	13.1.3	Segregação de redes
8.23	Novo	Filtragem da *web*
8.24	10.1.1, 10.1.2	Uso de criptografia
8.25	14.2.1	Ciclo de vida de desenvolvimento seguro
8.26	14.1.2, 14.1.3	Requisitos de segurança da aplicação
8.27	14.2.5	Princípios de arquitetura e engenharia de sistemas seguros
8.28	Novo	Codificação segura
8.29	14.2.8, 14.2.9	Testes de segurança em desenvolvimento e aceitação
8.30	14.2.7	Desenvolvimento terceirizado
8.31	12.1.4, 14.2.6	Separação dos ambientes de desenvolvimento, teste e produção
8.32	12.1.2, 14.2.2, 14.2.3, 14.2.4	Gestão de mudanças
8.33	14.3.1	Informações de testes
8.34	12.7.1	Proteção de sistemas de informação durante os testes de auditoria

A Tabela B.2 fornece a correspondência de controles especificados na ABNT NBR ISO/IEC 27002:2013 com os deste documento.

Tabela B.2 – Correspondência entre os controles da ABNT NBR ISO/IEC 27002:2013 e os controles deste documento (continua)

ABNT NBR ISO/IEC 27002:2013 Identificador de controle	ABNT NBR ISO/IEC 27002 Identificador de controle	Nome de controle de acordo com a ABNT NBR ISO/IEC 27002:2013
5		Políticas de segurança da informação
5.1		Orientação da direção para segurança da informação
5.1.1	5.1	Políticas de segurança da informação
5.1.2	5.1	Análise crítica das políticas para segurança da informação
6		Organização da segurança da informação
6.1		Organização interna
6.1.1	5.2	Responsabilidades e papéis da segurança da informação
6.1.2	5.3	Segregação de funções
6.1.3	5.5	Contato com autoridades
6.1.4	5.6	Contato com grupos especiais
6.1.5	5.8	Segurança da informação no gerenciamento de projetos
6.2		Dispositivos móveis e trabalho remoto
6.2.1	8.1	Política para uso de dispositivo móvel
6.2.2	6.7	Trabalho remoto
7		Segurança em recursos humanos
7.1		Antes da contratação
7.1.1	6.1	Seleção
7.1.2	6.2	Termos e condições de contratação
7.2		Durante a contratação
7.2.1	5.4	Responsabilidades da Direção
7.2.2	6.3	Conscientização, educação e treinamento em segurança da informação
7.2.3	6.4	Processo disciplinar
7.3		Encerramento e mudança de contratação
7.3.1	6.5	Responsabilidades pelo encerramento ou mudança da contratação
8		Gestão de ativos
8.1		Responsabilidade pelos ativos
8.1.1	5.9	Inventário dos ativos

Tabela B.2 (continuação)

ABNT NBR ISO/IEC 27002:2013 Identificador de controle	ABNT NBR ISO/IEC 27002 Identificador de controle	Nome de controle de acordo com a ABNT NBR ISO/IEC 27002:2013
8.1.2	5.9	Proprietário dos ativos
8.1.3	5.10	Uso aceitável dos ativos
8.1.4	5.11	Devolução de ativos
8.2		Classificação da informação
8.2.1	5.12	Classificação da informação
8.2.2	5.13	Rótulos e tratamento da informação
8.2.3	5.10	Tratamento dos ativos
8.3		Tratamento de mídias
8.3.1	7.10	Gerenciamento de mídias removíveis
8.3.2	7.10	Descarte de mídias
8.3.3	7.10	Transferência física de mídias
9		Controle de acesso
9.1		Requisitos do negócio para controle de acesso
9.1.1	5.15	Política de controle de acesso
9.1.2	5.15	Acesso às redes e aos serviços de rede
9.2		Gerenciamento de acesso do usuário
9.2.1	5.16	Registro e cancelamento de usuário
9.2.2	5.18	Provisionamento para acesso de usuário
9.2.3	8.2	Gerenciamento de direitos de acesso privilegiado
9.2.4	5.17	Gerenciamento da informação de autenticação secreta de usuários
9.2.5	5.18	Análise crítica dos direitos de acesso de usuário
9.2.6	5.18	Retirada ou ajuste dos direitos de acesso
9.3		Responsabilidades dos usuários
9.3.1	5.17	Uso da informação de autenticação secreta
9.4		Controle de acesso ao sistema e à aplicação
9.4.1	8.3	Restrição de acesso à informação
9.4.2	8.5	Procedimentos seguros de entrada no sistema (*log on*)
9.4.3	5.17	Sistema de gerenciamento de senha
9.4.4	8.18	Uso de programas utilitários privilegiados

Tabela B.2 (continuação)

ABNT NBR ISO/IEC 27002:2013 Identificador de controle	ABNT NBR ISO/IEC 27002 Identificador de controle	Nome de controle de acordo com a ABNT NBR ISO/IEC 27002:2013
9.4.5	8.4	Controle de acesso ao código-fonte de programas
10		Criptografia
10.1		Controles criptográficos
10.1.1	8.24	Política para o uso de controles criptográficos
10.1.2	8.24	Gerenciamento de chaves
11		Segurança física e do ambiente
11.1		Áreas seguras
11.1.1	7.1	Perímetro de segurança física
11.1.2	7.2	Controles de entrada física
11.1.3	7.3	Segurança em escritórios, salas e instalações
11.1.4	7.5	Proteção contra ameaças externas e do meio ambiente
11.1.5	7.6	Trabalhando em áreas seguras
11.1.6	7.2	Áreas de entrega e de carregamento
11.2		Equipamento
11.2.1	7.8	Localização e proteção do equipamento
11.2.2	7.11	Utilidades
11.2.3	7.12	Segurança do cabeamento
11.2.4	7.13	Manutenção dos equipamentos
11.2.5	7.10	Remoção de ativos
11.2.6	7.9	Segurança de equipamentos e ativos fora das dependências da organização
11.2.7	7.14	Reutilização ou descarte seguro de equipamentos
11.2.8	8.1	Equipamento de usuário sem monitoração
11.2.9	7.7	Política de mesa limpa e tela limpa
12		Segurança nas operações
12.1		Responsabilidades e procedimentos operacionais
12.1.1	5.37	Documentação dos procedimentos de operação
12.1.2	8.32	Gestão de mudanças
12.1.3	8.6	Gestão de capacidade

Tabela B.2 (continuação)

ABNT NBR ISO/IEC 27002:2013 Identificador de controle	ABNT NBR ISO/IEC 27002 Identificador de controle	Nome de controle de acordo com a ABNT NBR ISO/IEC 27002:2013
12.1.4	8.31	Separação dos ambientes de desenvolvimento, teste e produção
12.2		Proteção contra *malware*
12.2.1	8.7	Controles contra *malware*
12.3		Cópias de segurança
12.3.1	8.13	Cópia de segurança das informações
12.4		Registro e monitoramento
12.4.1	8.15	Registro de eventos
12.4.2	8.15	Proteção das informações dos registros de evento (*logs*)
12.4.3	8.15	Registros de eventos (*log)* de administrador e operador
12.4.4	8.17	Sincronização dos relógios
12.5		Controle de *software* operacional
12.5.1	8.19	Instalação de *software* nos sistemas operacionais
12.6		Gestão de vulnerabilidades técnicas
12.6.1	8.8	Gestão de vulnerabilidades técnicas
12.6.2	8.19	Restrições quanto à instalação de *software*
12.7		Considerações quanto à auditoria de sistemas de informação
12.7.1	8.34	Controles de auditoria de sistemas de informação
13		Segurança nas comunicações
13.1		Gerenciamento da segurança em redes
13.1.1	8.20	Controles de redes
13.1.2	8.21	Segurança dos serviços de rede
13.1.3	8.22	Segregação de redes
13.2		Transferência de informação
13.2.1	5.14	Políticas e procedimentos para transferência de informações
13.2.2	5.14	Acordos para transferência de informações
13.2.3	5.14	Mensagens eletrônicas
13.2.4	6.6	Acordos de confidencialidade e não divulgação

Tabela B.2 (continuação)

ABNT NBR ISO/IEC 27002:2013 Identificador de controle	ABNT NBR ISO/IEC 27002 Identificador de controle	Nome de controle de acordo com a ABNT NBR ISO/IEC 27002:2013
14		Aquisição, desenvolvimento e manutenção de sistemas
14.1		Requisitos de segurança de sistemas de informação
14.1.1	5.8	Análise e especificação dos requisitos de segurança da informação
14.1.2	8.26	Serviços de aplicação seguros em redes públicas
14.1.3	8.26	Protegendo as transações nos aplicativos de serviços
14.2		Segurança em processos de desenvolvimento e de suporte
14.2.1	8.25	Política de desenvolvimento seguro
14.2.2	8.32	Procedimentos para controle de mudanças de sistemas
14.2.3	8.32	Análise crítica técnica das aplicações após mudanças nas plataformas operacionais
14.2.4	8.32	Restrições sobre mudanças em pacotes de *software*
14.2.5	8.27	Princípios para projetar sistemas seguros
14.2.6	8.31	Ambiente seguro para desenvolvimento
14.2.7	8.30	Desenvolvimento terceirizado
14.2.8	8.29	Teste de segurança do sistema
14.2.9	8.29	Teste de aceitação de sistemas
14.3		Dados para teste
14.3.1	8.33	Proteção dos dados para teste
15		Relacionamento na cadeia de suprimento
15.1		Segurança da informação na cadeia de suprimento
15.1.1	5.19	Política de segurança da informação no relacionamento com fornecedores
15.1.2	5.20	Identificando segurança da informação nos acordos com fornecedores
15.1.3	5.21	Cadeia de suprimento na tecnologia da informação e comunicação
15.2		Gerenciamento da entrega do serviço do fornecedor

Tabela B.2 (continuação)

ABNT NBR ISO/IEC 27002:2013 Identificador de controle	ABNT NBR ISO/IEC 27002 Identificador de controle	Nome de controle de acordo com a ABNT NBR ISO/IEC 27002:2013
15.2.1	5.22	Monitoramento e análise crítica de serviços com fornecedores
15.2.2	5.22	Gerenciamento de mudanças para serviços com fornecedores
16		Gestão de incidentes de segurança da informação
16.1		Gestão de incidentes de segurança da informação e melhorias
16.1.1	5.24	Responsabilidades e procedimentos
16.1.2	6.8	Notificação de eventos de segurança da informação
16.1.3	6.8	Notificando fragilidades de segurança da informação
16.1.4	5.25	Avaliação e decisão dos eventos de segurança da informação
16.1.5	5.26	Resposta aos incidentes de segurança da informação
16.1.6	5.27	Aprendendo com os incidentes de segurança da informação
16.1.7	5.28	Coleta de evidências
17		Aspectos da segurança da informação na gestão da continuidade do negócio
17.1		Continuidade da segurança da informação
17.1.1	5.29	Planejando a continuidade da segurança da informação
17.1.2	5.29	Implementando a continuidade da segurança da informação
17.1.3	5.29	Verificação, análise crítica e avaliação da continuidade da segurança da informação
17.2		Redundâncias
17.2.1	8.14	Disponibilidade dos recursos de processamento da informação
18		Conformidade
18.1		Conformidade com requisitos legais e contratuais
18.1.1	5.31	Identificação da legislação aplicável e de requisitos contratuais

Tabela B.2 (conclusão)

ABNT NBR ISO/IEC 27002:2013 Identificador de controle	**ABNT NBR ISO/IEC 27002 Identificador de controle**	**Nome de controle de acordo com a ABNT NBR ISO/IEC 27002:2013**
18.1.2	5.32	Direitos de propriedade intelectual
18.1.3	5.33	Proteção de registros
18.1.4	5.34	Proteção e privacidade de informações de identificação pessoal
18.1.5	5.31	Regulamentação de controles de criptografia
18.2		Análise crítica da segurança da informação
18.2.1	5.35	Análise crítica independente da segurança da informação
18.2.2	5.36	Conformidade com as políticas e normas de segurança da informação
18.2.3	5.36, 8.8	Análise crítica da conformidade técnica

Bibliografia

[1] ABNT NBR ISO 9000, *Sistemas de gestão da qualidade – Fundamentos e vocabulário*

[2] ISO/IEC 11770 (*all parts*), *Information security – Key management*

[3] ISO/IEC 15408 (*all parts*), *Information technology – Security techniques – Evaluation criteria for IT security*

[4] ISO 15489 (*all parts*), *Information and documentation – Records management*

[5] ABNT NBR ISO/IEC 17788, *Tecnologia da informação – Computação em nuvem – Visão geral e vocabulário*

[6] ISO/IEC 17789, *Information technology – Cloud computing – Reference architecture*

[7] ISO/IEC 19086 (*all parts*), *Cloud computing – Service level agreement (SLA) framework*

[8] ISO/IEC 19770 (*all parts*), *Information technology – IT asset management*

[9] ISO/IEC 19941, *Information technology – Cloud computing – Interoperability and portability*

[10] ISO/IEC 20889, *Privacy enhancing data de-identification terminology and classification of techniques*

[11] ABNT NBR ISO 21500, *Gerenciamento de projeto, programa e portfólio – Contexto e conceitos*

[12] ABNT NBR ISO 21502, *Gerenciamento de projetos, programas e portfólios – Orientação sobre gerenciamento de projetos*

[13] ABNT NBR ISO 22301, *Segurança e resiliência – Sistema de gestão de continuidade de negócios – Requisitos*

[14] ABNT NBR ISO 22313, *Segurança e resiliência – Sistemas de gestão de continuidade de negócios – Orientações para o uso da ABNT NBR ISO 22301*

[15] ABNT ISO/TS 22317, *Segurança da sociedade – Sistemas de gestão de continuidade de negócios – Diretrizes para análise de impacto nos negócios (BIA)*

[16] ISO 22396, *Security and resilience – Community resilience – Guidelines for information exchange between organizations*

[17] ISO/IEC/TS 23167, *Information technology – Cloud computing – Common technologies and techniques*

[18] ISO/IEC 23751:–[2)], *Information technology – Cloud computing and distributed platforms – Data sharing agreement (DSA) framework*

[19] ISO/IEC 24760 (*all parts*), *IT Security and Privacy – A framework for identity management*

[20] ABNT NBR ISO/IEC 27001:2013, *Tecnologia da Informação – Técnicas de segurança – Sistemas de gestão da segurança da informação– Requisitos*

[21] ABNT NBR ISO/IEC 27005, *Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação*

[22] ABNT NBR ISO/IEC 27007, *Segurança da informação, segurança cibernética e proteção da privacidade – Diretrizes para auditoria de sistemas de gestão da segurança da informação*

[23] ISO/IEC/TS 27008, *Information technology – Security techniques – Guidelines for the assessment of information security controls*

[24] ISO/IEC 27011, *Information technology – Security techniques – Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations*

[25] ISO/IEC/TR 27016, *Information technology – Security techniques – Information security management – Organizational economics*

[26] ABNT NBR ISO/IEC 27017, *Tecnologia da informação – Técnicas de segurança – Código de prática para controles de segurança da informação com base ABNT NBR ISO/IEC 27002 para serviços em nuvem*

[27] ABNT NBR ISO/IEC 27018, *Tecnologia da informação – Técnicas de segurança – Código de prática para proteção de dados pessoais (DP) em nuvens públicas que atuam como operadores de DP*

[28] ISO/IEC 27019, *Information technology – Security techniques – Information security controls for the energy utility industry*

[29] ISO/IEC 27031, *Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity*

[30] ISO/IEC 27033 (*all parts*), *Information technology – Security techniques – Network security*

[31] ISO/IEC 27034 (*all parts*), *Information technology – Application security*

[32] ISO/IEC 27035 (*all parts*), *Information technology – Security techniques – Information security incident management*

[33] ISO/IEC 27036 (*all parts*), *Information technology – Security techniques – Information security for supplier relationships*

[34] ABNT NBR ISO/IEC 27037, *Tecnologia da informação – Técnicas de segurança – Diretrizes para identificação, coleta, aquisição e preservação de evidência digital*

[35] ISO/IEC 27040, *Information technology – Security techniques – Storage security*

[36] ISO/IEC 27050 (*all parts*), *Information technology – Electronic discovery*

[37] ISO/IEC/TS 27110, *Information technology, cybersecurity and privacy protection – Cybersecurity framework development guidelines*

[38] ABNT NBR ISO/IEC 27701, *Técnicas de segurança – Extensão das ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação – Requisitos e diretrizes*

[39] ABNT NBR ISO 27799, *Informática em saúde – Gestão de segurança da informação em saúde utilizando a ISO/IEC 27002*

[40] ABNT NBR ISO/IEC 29100, *Tecnologia da informação – Técnicas de segurança – Estrutura de Privacidade*

[41] ISO/IEC 29115, *Information technology – Security techniques – Entity authentication assurance framework*

[42] ABNT NBR ISO/IEC 29134, *Tecnologia da informação – Técnicas de segurança – Avaliação de impacto de privacidade – Diretrizes*

[43] ISO/IEC 29146, *Information technology – Security techniques – A framework for access management*

[44] ISO/IEC 29147, *Information technology – Security techniques – Vulnerability disclosure*

[45] ISO 30000, *Ships and marine technology – Ship recycling management systems – Specifications for management systems for safe and environmentally sound ship recycling facilities*

[46] ISO/IEC 30111, *Information technology – Security techniques – Vulnerability handling processes*

[47] ABNT NBR ISO 31000:2018, *Gestão de riscos – Diretrizes*

[48] ABNT NBR IEC 31010, *Gestão de riscos – Técnicas para o processo de avaliação de riscos*

[49] ISO/IEC 22123 (*all parts*), *Information technology – Cloud computing*

[50] ISO/IEC 27555, *Information security, cybersecurity and privacy protection – Guidelines on personally identifiable information deletion*

[51] Information Security Forum (ISF). The ISF Standard of Good Practice for Information Security 2020, August 2018. Available at https: /www.securityforum.org/tool/standard-of-good-practice-for-information-security-2020/

[52] ITIL® Foundation, ITIL 4 edition, AXELOS, February 2019, ISBN: 9780113316076

[53] National Institute of Standards and Technology (NIST), SP 800-53B, Control Baselines for Information Systems and Organizations, Revision 5 (Draft). July 2020 [viewed 2020-07-31]. Available at https://doi.org/10.6028/NIST.SP.800-53B-draft

[54] National Institute of Standards and Technology (NIST), SP 800-37, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, Revision 2. December 2018 [viewed 2020-07-31]. Available at https://doi.org/10.6028/NIST.SP.800-37r2

[55] Open Web Application Security Project (OWASP). OWASP Top Ten - 2017, The Ten Most Critical Web Application Security Risks, 2017 [viewed 2020-07-31]. Available at https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/

[56] Open Web Application Security Project (OWASP). OWASP Developer Guide, [online] [viewed 2020-10-22]. Available at https://github.com/OWASP/DevGuide

[57] National Institute of Standards and Technology (NIST), SP 800-63B, Digital Identity Guidelines; Authentication and Lifecycle Management. February 2020 [viewed 2020-07-31]. Available at https://doi.org/10.6028/NIST.SP.800-63b

[58] OASIS, Structured Threat Information Expression. Available at https://www.oasis-open.org/standards#stix2.0

[59] OASIS, Trusted Automated Exchange of Indicator Information. Available at https://www.oasis-open.org/standards#taxii2.0