



GUIA ORIENTATIVO DE SEGURANÇA CIBERNÉTICA PARA PRESTADORAS DE SERVIÇOS DE TELECOMUNICAÇÕES

NÍVEL BÁSICO – Versão 1.0

Outubro/2023

Sumário

Lista de Abreviaturas, Acrônimos e Siglas.....	2
Apresentação e Objetivo.....	3
Capítulo 1: Inventário de Ativos.....	6
Capítulo 2: Proteção de Dados.....	10
Capítulo 3: Configuração Segura de Ativos e Gestão de Vulnerabilidades	13
Capítulo 4: Controle de Acesso e Contas	18
Capítulo 5: Monitoramento de Atividades e Gestão de Registros de Auditoria	22
Capítulo 6: Backup e Recuperação de Dados.....	26
Capítulo 7: Conscientização dos Funcionários sobre Segurança Cibernética	29
Capítulo 8: Conscientização dos Consumidores sobre Segurança Cibernética	33
Capítulo 9: Segurança Física	36
Capítulo 10: Plano de Resposta a Incidentes.....	39
Capítulo 11: Política de Segurança Cibernética	41
Considerações Finais	44
Checklist.....	46
Referências.....	47
Glossário	50
Anexo 1 - Resumo dos Objetivos do Guia.....	56
Anexo 2 - Resumo das Medidas do Guia	57

Lista de Abreviaturas, Acrônimos e Siglas

- ABNT - Associação Brasileira de Normas Técnicas
- CERT.br - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
- CIS - *Center for Internet Security*
- DNS - *Domain Name System*
- GRC - Governança, Riscos e Compliance
- GSI/PR - Gabinete de Segurança Institucional da Presidência da República
- HTTP - *Hypertext Transfer Protocol*
- HTTPS - *Hypertext Transfer Protocol Secure*
- IDS - Sistema de Detecção de Intrusão
- IoT - Internet das Coisas
- IPS - Sistema de Prevenção de Intrusão
- IPv4 - *Internet Protocol version 4*
- IPv6 - *Internet Protocol version 6*
- ISO – *International Organization for Standardization*
- MDM - *Mobile Device Management*
- MFA - Autenticação Multifator
- NaaS - *Network-as-a-Service*
- NBR ISO/IEC - Norma Brasileira ISO/IEC
- NIST - *National Institute of Standards and Technology*
- PPSI - Programa de Privacidade e Segurança da Informação
- SCADA - *Supervisory Control and Data Acquisition*
- SGD/MGI - Secretaria-Geral de Desburocratização, Gestão e Governo Digital do Ministério da Gestão Interna
- SIEM - Sistemas de Gerenciamento de Informações e Eventos de Segurança
- SSH - *Secure Shell*
- SSO - *Single Sign On*
- Telnet - *Teletype Network*
- TI – Tecnologia da Informação
- TICs - Tecnologias de Informação e Comunicação
- UBA - Análise de Comportamento do Usuário
- URL - *Uniform Resource Locator*

Apresentação e Objetivo

O presente guia tem como propósito orientar as prestadoras de serviços de telecomunicações na proteção de suas redes, sistemas e dados diante das ameaças cibernéticas. Ele oferece diretrizes e práticas recomendadas para a salvaguarda de ativos corporativos, incluindo redes, sistemas e dados. Dada a relevância dos serviços prestados pelas empresas do setor de telecomunicações e a vasta quantidade de dados que gerenciam, elas frequentemente se tornam alvos de ataques cibernéticos. Assim, torna-se imperativo que tais empresas implementem medidas robustas de segurança para suas redes, sistemas e dados, bem como de resiliência para garantir a continuidade do serviço prestado no caso de ocorrência de um incidente

No cenário digital contemporâneo, a segurança cibernética emerge como uma preocupação preponderante. O aumento na frequência de ataques cibernéticos [1] e o valor intrínseco dos dados na rede sublinham a necessidade de proteção informacional para organizações de variados portes e segmentos, incluindo as prestadoras de telecomunicações.

Este guia visa a materializar as diretrizes estabelecidas pelo Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações (R-Ciber), aprovado pela Resolução nº 740, de 21 de dezembro de 2020 [2], enfatizando a adoção de boas práticas e padrões nacionais e internacionais relacionados à segurança cibernética. Além disso, promove a disseminação da cultura de segurança cibernética e a utilização segura e sustentável das redes e serviços de telecomunicações. Destaca-se, neste documento, a importância das políticas relacionadas aos principais assuntos de segurança cibernética na manutenção da confidencialidade, integridade, disponibilidade das informações, para proteger consumidores, colaboradores e prestadores de serviços, bem como garantir a continuidade operacional das empresas.

O Guia foi elaborado de forma colaborativa no âmbito do Setor de Telecomunicações, utilizando-se do fórum do Grupo de Estudos do Exercício Guardião Cibernético 5.0 (EGC 5.0), bem como da estrutura do Grupo Técnico de Segurança Cibernética e Gestão de Riscos de Infraestrutura Crítica (GT-Ciber) da Anatel e construído com base nas deliberações do GT-Ciber. O GT-Ciber foi constituído pelo R-Ciber, possuindo uma série de atribuições relacionadas ao acompanhamento da Política de Segurança Cibernética e Gestão de Infraestrutura Crítica; à elaboração das definições complementares para implementação do R-Ciber; à conscientização,

capacitação, estudos e à interação com as Comissões Brasileiras de Comunicações (CBCs); dentre outras.

Destaca-se, aqui, especialmente a atribuição do GT-Ciber para “*propor ações e iniciativas a serem adotadas pelas prestadoras dispensadas do cumprimento das obrigações estabelecidas neste Regulamento, de forma que os princípios e diretrizes nele dispostas sejam seguidos*”, nos termos do art. 24, III, do R-Ciber, que dialoga especialmente com esse Guia de nível básico¹.

Para a elaboração técnica deste guia, buscou-se utilizar procedimentos e recomendações amplamente adotados por entidades privadas e públicas, em especial o Guia “Controles CIS Versão 8” do *Center for Internet Security* (CIS) [3]; o Guia de Aperfeiçoamento da Segurança Cibernética para Infraestrutura Crítica do *National Institute of Standards and Technology* (NIST), versão 1.1 [4]; as Normas Brasileiras ABNT NBR ISO/IEC 27001:2022 [5] e 27002:2022 [6]; as diretrizes da Portaria SGD/MGI nº 852, de 28 de março de 2023 [7], que dispõe sobre o Programa de Privacidade e Segurança da Informação (PPSI), bem como todos os guias e modelos; e o Glossário de Segurança da Informação, conforme a Portaria nº 93, de 18 de outubro de 2021, do Gabinete de Segurança Institucional da Presidência da República (GSI/PR)[8], e suas respectivas atualizações².

Ademais, o Guia Orientativo sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte da Autoridade Nacional de Proteção de Dados (ANPD) [9], e o seu respectivo *checklist*, serviram de inspiração para o desenvolvimento desse guia e constituem valiosa ferramenta para as prestadoras de serviço de telecomunicações, especialmente as Prestadoras de Pequeno Porte, no tocante à proteção de dados pessoais.

Por fim, ressalva-se que a Anatel e as organizações que participaram do trabalho de desenvolvimento deste Guia:

- a) não representam, tampouco se manifestam em nome do CIS, NIST, ABNT, ISO, PPSI ou GSI/PR e vice-versa;
- b) não são coautora das publicações internacionais abordadas;
- c) não assumem nenhuma responsabilidade administrativa, técnica ou jurídica pelo uso ou pela interpretação inadequados, fragmentados ou parciais do presente Guia;

Caso o leitor deseje se certificar de que o Guia atende integralmente os requisitos das publicações do CIS, NIST, Associação Brasileira de Normas Técnicas (ABNT) ou *International*

¹ A capa foi confeccionada com os recursos de Freepik.com.

² Algumas referências foram traduzidas de forma livre pelos técnicos envolvidos no desenvolvimento do documento, com propósitos educativos e não comerciais a fim de difundir tais conhecimentos para o bem público.

Organization for Standardization (ISO), deverá consultar diretamente as fontes oficiais de informação ofertadas pelas referidas instituições.

Agradecimento especial ao CIS, NIST, ABNT, ISO, PPSI da Secretaria de Governo Digital e GSI/PR pelas valiosas contribuições para a promoção da segurança cibernética.

Capítulo 1: Inventário de Ativos

Gerenciar (inventariar, rastrear e corrigir) os ativos institucionais e softwares, com o objetivo de identificar precisamente quais necessitam ser monitorados, bloqueados e/ou protegidos dentro da empresa, mapeando os ativos não autorizados para uma possível remoção ou remediação futura.

As prestadoras de telecomunicações são um alvo cada vez mais comum para os hackers e criminosos cibernéticos [10]. É essencial que essas empresas compreendam a importância da segurança cibernética e adotem medidas proativas para proteger seus dados e sistemas.

Neste capítulo, vamos discutir a importância do inventário de ativos, do processo de gestão ativa para prestadoras de telecomunicações e iniciativas básicas para se estruturar tal gestão.

Como objetivo desse item pode-se destacar:

Estabelecer e manter uma política de gestão de ativos de para inventariar, rastrear e corrigir todos os ativos corporativos, sejam eles dados, dispositivos de usuário, de rede, Internet das coisas (IoT), dispositivos de rede, servidores ou softwares (sistemas operacionais ou aplicações), independentemente de sua conexão ser física, virtual, remota ou em nuvem. Esse controle permite identificar e tratar ativos não autorizados e garantir que apenas softwares aprovados sejam instalados e executados. Isso também ajudará na identificação de ativos não autorizados e não gerenciados para removê-los ou remediá-los. [3], [4], [5] e [6].

Como inspiração inicial para tal processo pode-se utilizar os conceitos, orientações e melhores práticas do Modelo de Política de Gestão de Ativos do Programa de Privacidade e Segurança da Informação (PPSI) [11].

Por que é importante estabelecer e manter um processo de gestão de ativos?

As empresas precisam ter conhecimento e gestão adequada de seus ativos para garantir a segurança, responder a incidentes e recuperar sistemas. Saber quais dados são vitais e onde estão armazenados permite aplicar controles de segurança eficazes. Atacantes externos constantemente buscam ativos vulneráveis, seja localmente ou na nuvem. Ativos mal configurados ou não identificados internamente podem ser explorados por *malwares* ou e-mails

maliciosos. Qualquer ativo conectado à rede corporativa, como sistemas temporários ou redes de convidados, deve ser identificado ou isolado para manter a segurança operacional.

Como medidas básicas de segurança indicadas para esse processo destacam-se:

1.1 Estabelecer e manter um inventário detalhado de ativos corporativos

Mantenha um registro meticuloso, atual e abrangente de todos os ativos empresariais com capacidade para armazenar ou processar informações. Este registro deve incluir, por exemplo: (i) Dispositivos de usuário final, abrangendo equipamentos portáteis e móveis; (ii) Equipamentos de rede; (iii) Dispositivos não computacionais ou relacionados à Internet das Coisas (IoT); (iv) Servidores. Para cada ativo, o inventário deve documentar: (i) Endereço de rede (caso seja estático); (ii) Endereço físico do hardware; (iii) Nome do dispositivo; (iv) Proprietário do ativo de dados; (v) Departamento associado ao ativo; e (vi) Confirmação de autorização para conexão à rede corporativa.

Para a gestão de dispositivos móveis de usuário final, considere a utilização de ferramentas de Gestão de Dispositivos Móveis (MDM) quando pertinente. O escopo deste inventário abrange ativos ligados à infraestrutura de maneira física, virtual, remota e em ambientes de computação em nuvem. Adicionalmente, engloba ativos que se conectam regularmente à rede corporativa, mesmo que não estejam sob supervisão direta da organização.

É imperativo revisar e atualizar o registro de todos os ativos empresariais ao menos semestralmente, ou em intervalos mais curtos conforme necessário.

1.2 Tratar ativos não autorizados

Garanta a implementação de um procedimento semanal para gerenciar ativos não autorizados. A organização pode optar por desvincular o ativo da rede, proibir sua conexão remota à infraestrutura ou submeter o ativo a um regime de quarentena.

1.3 Estabelecer e manter um inventário de software

Institua e conserve um registro meticuloso de todos os softwares licenciados presentes nos ativos empresariais. O catálogo de software deve registrar: (i) Título do software; (ii) Editor ou desenvolvedor; (iii) Data de instalação ou início de uso; e (iv) Finalidade empresarial do software. Quando pertinente, o registro deve também incluir: (i) *Uniform Resource Locator* (URL); (ii) Loja(s) de aplicativos de origem; (iii) Versão(ões) do software; (iv) Mecanismo de implantação; e (v) Data de desativação.

É essencial revisar e atualizar o catálogo de software ao menos semestralmente, ou em intervalos mais curtos conforme necessário.

1.4 Assegurar que o software autorizado seja atualmente suportado

Garanta que somente softwares com suporte vigente sejam categorizados como autorizados no registro de software dos ativos empresariais. Caso um software não possua suporte do fornecedor, mas seja imprescindível para a execução das atividades empresariais, é necessário elaborar uma exceção documentada, detalhando as medidas de mitigação adotadas e a aceitação do risco remanescente. Qualquer software sem suporte que não possua uma exceção documentada deve ser classificado como não autorizado. É imperativo revisar o registro de software para confirmar o suporte dele ao menos mensalmente, ou em intervalos mais curtos conforme necessário.

1.5 Tratar o software não autorizado

Garanta que softwares não autorizados sejam desativados dos ativos empresariais ou, alternativamente, possuam uma exceção devidamente documentada. A revisão deste procedimento deve ser realizada ao menos mensalmente ou em intervalos mais curtos, conforme a necessidade.

1.6 Estabelecer e manter um inventário de contas

Institua e conserve um registro meticuloso de todas as contas gerenciadas dentro da organização. Este registro deve abranger tanto contas de usuários comuns quanto contas administrativas. Para cada conta, o inventário deve documentar: (i) Nome completo do titular; (ii) Nome de usuário associado; (iii) Data de ativação da conta; (iv) Data de término ou desativação (quando aplicável); e (v) Departamento ao qual pertence.

É essencial que, em um ciclo recorrente, preferencialmente ao menos a cada trimestre ou em intervalos mais curtos, conforme necessário, se verifique e confirme a autorização de todas as contas ativas.

1.7 Estabelecer e manter um inventário de provedores de serviços

Institua e preserve um registro sistemático dos provedores de serviço associados à organização. Este catálogo deve: (i) Enumerar todos os provedores de serviços reconhecidos; (ii) Fornecer uma classificação para cada provedor (ex: provedores de infraestrutura; provedores de software; provedores de suporte e manutenção, dentre outros); (iii) Designar um representante da empresa como ponto de contato para cada provedor de serviços.

É imperativo revisar e atualizar este registro anualmente. Além disso, atualizações devem ser realizadas sempre que houver alterações substanciais na organização que possam influenciar esta prática de segurança.

Conclusão

O conhecimento e gestão adequada dos ativos corporativos é parte fundamental para garantir a segurança, responder a incidentes e recuperar sistemas. Dessa forma, estabelecer e manter um processo de gestão ativa para inventariar, rastrear e corrigir todos os ativos corporativos contribui na melhoria da segurança cibernética.

Capítulo 2: Proteção de Dados

Desenvolva processos e controles técnicos para identificar, classificar, manusear com segurança, reter e descartar dados.

Desenvolver processos e controles técnicos para identificar, classificar, manusear com segurança, reter e descartar dados é fundamental para garantir a integridade, confidencialidade e disponibilidade das informações em uma organização. Em um cenário no qual a quantidade de dados gerados cresce exponencialmente, é imprescindível que as empresas tenham mecanismos robustos para gerenciar essas informações. Uma gestão inadequada pode resultar em vazamentos de dados, comprometendo a privacidade de indivíduos e expondo a organização a riscos legais, financeiros e de reputação.

Como objetivo de tal item pode-se destacar:

Estabelecer e manter uma política de proteção de dados [3], [4], [5] e [6].
--

Por que é necessário criar tal processo?

Os dados corporativos ultrapassam as fronteiras tradicionais das empresas, estando distribuídos em nuvens, dispositivos portáteis e em ambientes de trabalho remoto, podendo ser compartilhados globalmente com parceiros e serviços online. Além da importância intrínseca de dados financeiros, propriedade intelectual e de dados pessoais dos consumidores, as empresas enfrentam regulamentações internacionais rigorosas para a proteção de dados pessoais. As medidas de proteção para salvaguardar os dados pessoais de consumidores e dos funcionários das prestadoras não pode se limitar à utilização de criptografia, envolvendo necessariamente uma gestão adequada ao longo de todo o seu ciclo de vida, configurando um desafio complexo para qualquer empresa.

Quando invasores acessam a infraestrutura de uma empresa, geralmente sua prioridade é localizar e extrair dados valiosos. Muitas organizações não percebem a saída de informações sensíveis devido à falta de monitoramento adequado. Os ataques podem variar desde o roubo físico de dispositivos até invasões em sistemas de parceiros ou em sistemas de controle como o SCADA (Sistemas de Supervisão e Aquisição de Dados). A perda ou comprometimento de dados, muitas vezes, não é resultado de ações maliciosas diretas, mas de má gestão e erros humanos.

Assim, a criptografia, tanto de dados em trânsito quanto em repouso, torna-se essencial não apenas como medida de segurança, mas também como exigência regulatória.

Como principais medidas para tal processo destacam-se:

2.1 Estabelecer e manter um processo de gestão de dados.

Institua e preserve um protocolo sistemático para a gestão de dados. Dentro deste protocolo, aborde: (i) A natureza sensível dos dados; (ii) A identificação do responsável pelos dados; (iii) As práticas de manipulação dos dados; (iv) Os períodos estabelecidos para a retenção dos dados; e (v) As diretrizes para o descarte adequado dos dados.

Estas considerações devem ser fundamentadas em padrões estabelecidos de sensibilidade e retenção pertinentes à organização. É essencial revisar e atualizar este protocolo anualmente. Adicionalmente, modificações devem ser realizadas sempre que houver alterações substanciais na organização que possam influenciar esta prática de segurança.

2.2 Estabelecer e manter um inventário de dados.

Institua e conserve um registro sistemático de dados, fundamentado no protocolo de gestão de dados da organização. Prioritariamente, é imperativo catalogar os dados de natureza sensível. Este inventário deve ser revisado e atualizado, pelo menos, anualmente, dando especial atenção aos dados sensíveis.

2.3 Configurar listas de controle de acesso a dados

Estabeleça listas de controle de acesso aos dados, fundamentadas na necessidade de conhecimento específico do usuário. Implemente essas listas, frequentemente referidas como permissões de acesso, em sistemas de arquivos, bancos de dados e aplicações, tanto locais quanto remotas.

2.4 Aplicar retenção de dados

Mantenha os dados conforme estabelecido no protocolo de gestão de dados da organização. A política de retenção de dados deve especificar períodos mínimos e máximos de armazenamento.

2.5 Descartar dados com segurança

Elimine os dados de forma segura, em conformidade com o protocolo de gestão de dados estabelecido pela organização. Assegure-se de que o procedimento e a técnica de eliminação estejam alinhados à natureza sensível dos respectivos dados.

2.6 Criptografar dados em dispositivos de usuário final.

Criptografe os dados em dispositivos de usuário final que armazenem informações de natureza sensível. Algumas soluções sugeridas para essa implementação incluem: *Windows BitLocker®*, *Apple FileVault®* e *Linux® dm-crypt*.

Conclusão

Resta clara a importância crítica de estabelecer e manter processos robustos e controles técnicos para a gestão adequada de dados e informações. Em um mundo digitalizado e interconectado, os dados não apenas representam ativos valiosos, mas também carregam riscos significativos se não forem adequadamente protegidos e gerenciados. A proliferação de dados em diversos ambientes, desde nuvens até dispositivos portáteis, exige uma abordagem holística de proteção.

Além das ameaças externas, as organizações devem estar atentas às vulnerabilidades internas, como erros humanos, que podem comprometer a integridade dos dados. A implementação de medidas como inventário de dados, listas de controle de acesso e criptografia são essenciais para garantir que os dados sejam acessados apenas por aqueles autorizados e que sejam mantidos seguros durante todo o seu ciclo de vida. Em resumo, a proteção de dados não é apenas uma necessidade técnica, mas uma responsabilidade ética e legal das organizações para com seus clientes e *stakeholders*.

Capítulo 3: Configuração Segura de Ativos e Gestão de Vulnerabilidades

Defina e mantenha a configuração segura de recursos empresariais (ex: dispositivos móveis; equipamentos de rede e servidores) e programas (ex: sistemas e aplicações). Além disso mantenha um processo de gestão de vulnerabilidades otimizando as configurações seguras dos ativos.

Manter seus sistemas e softwares com configuração segura é crucial para garantir a correta operação da sua empresa de telecomunicações. As melhores práticas sobre configurações seguras podem ajudar a minimizar as ameaças cibernéticas e ataques, protegendo seus sistemas. Neste capítulo, discutiremos as melhores práticas para manter seus recursos empresariais em segurança.

Como objetivo de tal item pode-se destacar:

Estabelecer e manter uma política de configuração segura de ativos e uma política de gestão de vulnerabilidades, bem como [3], [4], [5] e [6].

Como modelo inicial para tal processo pode-se utilizar os conceitos, orientações e melhores práticas do Guia de Gerenciamento de Vulnerabilidades do Programa de Privacidade e Segurança da Informação (PPSI) [12].

Por que é necessário criar tal processo?

As configurações padrão de ativos e softwares corporativos, fornecidas por fabricantes e revendedores, priorizam a facilidade de uso em detrimento da segurança. Isso pode incluir serviços e portas abertos, senhas padrão e software desnecessário, que se não alterados, podem ser vulneráveis. É essencial gerenciar e manter atualizações de segurança ao longo do ciclo de vida dos ativos, com um registro para compliance e auditorias. Provedores de serviços, comuns em empresas menores, muitas vezes não oferecem configurações seguras por padrão, deixando a responsabilidade de segurança para a empresa usuária. Mesmo após estabelecer configurações seguras, é crucial gerenciá-las continuamente, considerando atualizações, novas vulnerabilidades e ajustes operacionais. Dessa forma faz-se necessário manter um processo de configuração segura. 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.

Como principais medidas para tal processo destacam-se:

3.1 Estabelecer e manter um processo de configuração segura

Institua e preserve um protocolo para a configuração segura de ativos empresariais, abrangendo dispositivos de usuário final (tais como equipamentos portáteis e móveis), dispositivos não computacionais ou relacionados à Internet das Coisas (IoT), e servidores, bem como software, incluindo sistemas operacionais e aplicações. É essencial revisar e atualizar este protocolo anualmente ou sempre que houver alterações substanciais na organização que possam influenciar esta prática de segurança.

3.2 Estabelecer e manter um processo de configuração segura para a infraestrutura de rede

Institua e conserve um protocolo para a configuração segura de dispositivos de rede. É imperativo revisar e atualizar este protocolo anualmente ou sempre que houver alterações substanciais na organização que possam afetar esta prática de segurança.

3.3 Configurar o bloqueio automático de sessão nos ativos corporativos

Estabeleça um mecanismo de bloqueio automático nos ativos empresariais que seja ativado após um intervalo específico de inatividade. Em sistemas operacionais de uso comum, esse intervalo não deve ultrapassar 15 minutos. Já para dispositivos móveis destinados ao usuário final, o período estipulado não deve exceder 2 minutos.

3.4 Implementar e gerenciar um firewall nos servidores

Institua e administre um firewall nos servidores compatíveis. As soluções para essa implementação podem abranger um firewall virtual, um firewall integrado ao sistema operacional ou um agente de firewall provido por terceiros.

3.5 Implementar e gerenciar um firewall nos dispositivos de usuário final

Estabeleça e administre um firewall de host ou uma ferramenta de filtragem de portas nos dispositivos destinados ao usuário final. Adote uma regra padrão de negação que obstrua todo o tráfego, ressaltando apenas os serviços e portas que receberam autorização explícita.

3.6 Gerenciar com segurança os ativos e softwares corporativos

Administre os ativos e softwares empresariais de forma segura. Algumas soluções recomendadas para essa implementação abrangem a gestão de configuração através de métodos de controle de

versão da infraestrutura tratada como código (*version-controlled-infrastructure-as-code*) e o acesso a interfaces administrativas utilizando protocolos de rede seguros, tais como *Secure Shell* (SSH) e *Hypertext Transfer Protocol Secure* (HTTPS). Evite protocolos de gestão considerados inseguros, como Telnet (*Teletype Network*) e HTTP (*Hypertext Transfer Protocol*), salvo quando estritamente necessário para operações.

3.7 Gerenciar contas padrão nos ativos e softwares corporativos

Administre de forma apropriada as contas padrão presentes nos ativos e softwares empresariais, tais como "root", "administrador" e outras contas pré-configuradas por fornecedores. Algumas soluções recomendadas para essa implementação abrangem a desativação dessas contas padrão ou a sua configuração para que se tornem inoperantes.

3.8 Garantir o uso apenas de navegadores e clientes de e-mail suportados plenamente

Assegure-se de que somente navegadores e consumidores de e-mail com suporte integral sejam autorizados a operar dentro da organização, utilizando exclusivamente as versões mais atualizadas desses navegadores e consumidores de e-mail disponibilizadas pelo respectivo fornecedor.

3.9 Usar serviços de filtragem de DNS

Empregue serviços de filtragem de DNS (*Domain Name Service*) em todos os ativos empresariais com o objetivo de obstruir o acesso a domínios reconhecidamente maliciosos.

3.10 Instalar e manter um software *anti-malware*

Instale e mantenha um software *anti-malware* em todos os ativos corporativos.

3.11 Configurar atualizações automáticas de assinatura *anti-malware*

Configure atualizações automáticas para arquivos de assinatura *anti-malware* em todos os ativos corporativos.

3.12 Desabilitar a execução e reprodução automática para mídias removíveis

Desabilitar a funcionalidade de execução e reprodução automática para mídias removíveis.

3.13 Acelerar a transição completa para o IPv6 o mais breve possível

Com o esgotamento dos endereços IPv4, a adoção do protocolo IPv6³ nas redes e a sua adoção para a disponibilização de conteúdo tornam-se imperativas. Esta nova versão é essencial para dar suporte a tecnologias emergentes, como a Internet das Coisas (IoT), e para garantir a

³ <https://www.internetsociety.org/deploy360/ipv6/faq/>

interoperabilidade entre sistemas. Além disso, o IPv6 oferece funcionalidades avançadas que reforçam a segurança das redes e protegem seus usuários.

É importante destacar que mecanismos como o NAT (*Network Adresse Translation*), amplamente utilizados para contornar as limitações do IPv4, apresentam fragilidades. O NAT, ao traduzir endereços IP privados em públicos, pode introduzir complicações na rastreabilidade de sessões e potenciais vulnerabilidades de segurança. Além disso, esse mecanismo pode complicar a implementação de certos serviços e a análise de tráfego em redes. Portanto, a transição para o IPv6 não apenas alivia a escassez de endereços, mas também supera as fragilidades associadas ao uso prolongado do NAT no contexto do IPv4.

3.14 Estabelecer e manter um processo de gestão de vulnerabilidade

Institua e preserve um protocolo documentado para a gestão de vulnerabilidades relativas aos ativos empresariais. É essencial revisar e atualizar este protocolo anualmente ou sempre que houver alterações substanciais na organização que possam afetar esta prática de segurança.

3.15 Estabelecer e manter um processo de remediação

Desenvolva e mantenha uma estratégia de remediação baseada em risco, devidamente registrada em um processo formal de remediação, com revisões que ocorram mensalmente ou com maior frequência, conforme a necessidade.

Esta estratégia de remediação baseada em risco envolve a identificação das vulnerabilidades de acordo com seu grau de severidade e o potencial impacto nos ativos da organização. Prioriza-se a resolução das vulnerabilidades de maior risco, garantindo que os recursos sejam alocados de maneira eficaz para abordar as ameaças mais críticas.

Essa abordagem contribui para fortalecer a postura de segurança da organização, minimizando as vulnerabilidades que representam maiores ameaças e garantindo que ações de remediação sejam conduzidas de maneira ágil e eficiente.

3.16 Manter sistemas e aplicações atualizados (gestão automatizada de patches)

A manutenção da atualização dos sistemas e softwares é uma medida crítica para salvaguardar a segurança da organização. Vulnerabilidades conhecidas em sistemas e software desatualizados podem ser exploradas por atacantes, resultando na exposição de informações confidenciais.

É recomendável configurar os sistemas e softwares para receber atualizações de forma automática, assegurando que eles estejam sempre executando a versão mais recente e protegida contra ameaças conhecidas. Além disso, é aconselhável conduzir atualizações do sistema operacional e das aplicações em ativos corporativos por meio de um sistema de gestão

automatizada de patches, com uma frequência mensal ou até mesmo mais frequente, conforme necessário.

Conclusão

Manter seus sistemas e software com configuração segura e atualizada é uma das melhores práticas para proteger sua empresa de telecomunicações contra ameaças cibernéticas. Estabelecer e manter um processo de configuração segura para dispositivos de rede, configuração de bloqueio automático de sessão nos ativos corporativos, implementação e gerenciamento de firewall em servidores e dispositivos de usuários, dentre outras medidas podem minimizar as vulnerabilidades e garantir mais segurança a seus sistemas.

Capítulo 4: Controle de Acesso e Contas

Use processos e ferramentas para atribuir e gerenciar autorização de credenciais, bem como criar, atribuir, gerenciar e revogar credenciais de acesso e privilégios para contas de usuário, administrador e serviço para ativos e softwares corporativos.

É imperativo instituir mecanismos rigorosos de identificação, autenticação e autorização para assegurar a integridade das informações pertencentes as prestadoras de telecomunicações. Tais medidas são cruciais para prevenir violações de segurança da informação e quaisquer incursões não autorizadas que possam resultar em destruição, modificação, perda, furto ou divulgação inapropriada das informações. A ausência de tais controles de autorização, identificação e autenticação amplia consideravelmente o risco de acessos ilícitos e comprometimento da segurança dos sistemas de informação.

Senhas são um dos aspectos mais básicos e críticos da segurança cibernética. Elas servem como a primeira linha de defesa contra acesso não autorizado à sua rede e a informações confidenciais. Na mesma linha, a autenticação multifator (MFA) é uma camada adicional de segurança que ajuda a proteger as prestadoras de serviços de telecomunicações contra acessos não autorizados. A MFA exige que os usuários forneçam duas ou mais formas de autenticação antes de acessar sistemas ou contas, tornando o processo de autenticação mais robusto.

Neste capítulo, discutiremos algumas das melhores práticas para o gerenciamento de senhas e controle de acesso para ajudar a proteger as empresas contra ameaças cibernéticas, também discutindo a importância da MFA e como implementá-la nas organizações.

Como objetivo de tal item pode-se destacar:

Estabelecer e manter uma política de controle de acesso e contas para definir regras para acesso a diversos sistemas, equipamentos, instalações e informações com base nos requisitos comerciais e de segurança para obtenção de acesso. [3], [4], [5] e [6].

Como modelo inicial para tal política pode-se utilizar o Modelo de Política de Gestão de Controle de Acesso do Programa de Privacidade e Segurança da Informação (PPSI) [13].

Por que criar uma política de controle de acesso?

O acesso não autorizado a dados empresariais usando credenciais válidas é uma prática comum de hackers. Esse acesso pode ser obtido de diversas formas, como quebra de senhas fracas, contas desatualizadas, contas compartilhadas não modificadas por longos períodos, ou até mesmo por meio de engenharia social e *malware*. Contas com altos privilégios são especialmente visadas, pois permitem ações mais amplas no sistema. Além disso, contas de serviço, que muitas vezes são compartilhadas e pouco monitoradas, representam riscos. O registro e supervisão de contas são essenciais para a segurança e fazem parte de uma gestão eficaz de acesso e identidades.

Importante destacar que tal gestão de acesso assegura que os usuários acessem somente os recursos corporativos adequados às suas funções e que haja autenticação robusta para informações sensíveis. É essencial que as contas tenham apenas as permissões mínimas necessárias e que os direitos de acesso sejam consistentes por função.

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”.

Senhas por si só não são mais suficientes para proteger contra ameaças cibernéticas. Os cibercriminosos podem facilmente adivinhar ou quebrar senhas, ou até mesmo obtê-las por meio de ataques de *phishing*. Ao implementar a autenticação multifator (MFA), cria-se uma camada extra de proteção contra acesso não autorizado. Mesmo que um hacker obtenha a senha de um usuário, eles ainda precisam fornecer autenticação adicional para acessar sistemas ou contas críticas.

Como medidas básicas de segurança indicadas para auxiliar no controle de acesso:

4.1 Utilizar senhas fortes e exclusivas

Uma senha robusta é aquela que se mostra altamente resistente a tentativas de adivinhação ou violação por terceiros. De acordo com as melhores práticas de segurança, é recomendável que, no mínimo, as senhas tenham 8 caracteres para contas que utilizam autenticação multifator (MFA) e 14 caracteres para contas que não adotam essa camada adicional de segurança [2]. É importante evitar o uso de informações facilmente deduzíveis, como datas de nascimento, nomes de familiares ou frases comuns.

4.2 Exigir mudanças periódicas de senhas

A prática de atualizar regularmente as senhas é um elemento fundamental na administração de credenciais de acesso. Ao modificar as senhas de forma periódica, é possível mitigar o risco de um cibercriminoso obter acesso contínuo à rede. Recomenda-se considerar a implementação de uma

política que exija que os colaboradores atualizem suas senhas a cada 90 dias ou em intervalos de tempo ainda menores. Isso contribuirá para manter um ambiente de segurança mais robusto.

4.3 Não compartilhar senhas

É estritamente proibido compartilhar senhas com terceiros, mesmo quando se trata de colegas dentro da organização. Cada membro da equipe deve dispor de suas próprias credenciais de login exclusivas. Quando diversas pessoas necessitarem de acesso a uma mesma conta ou sistema, é recomendável considerar a implantação de um sistema que permita a criação de contas de usuário individuais, cada uma com níveis de acesso diferenciados. Isso assegurará um controle mais rigoroso e se alinhará com as práticas de segurança adequadas.

4.4 Não armazenar senhas em locais de fácil acesso

O hábito de armazenar senhas em locais de fácil acesso, como por exemplo, em um adesivo colado ao monitor do computador, é uma prática que, embora comum, apresenta sérios riscos de segurança. Caso um invasor obtenha acesso físico ao ambiente de trabalho, ele poderá facilmente adquirir acesso à rede simplesmente ao roubar uma senha dessa maneira. Tal prática deve ser evitada a todo custo, a fim de salvaguardar a integridade e confidencialidade dos sistemas e dados da organização.

4.5 Desabilitar contas inativas

Elimine ou inative todas as contas que permaneçam inativas por um período de 45 dias, quando essa ação for viável. Além disso, as contas que não tiverem suas senhas alteradas durante um intervalo de 90 dias também devem ser desabilitadas. Essa medida visa aprimorar a segurança e a eficiência na gestão das contas de usuário.

4.6 Limitar as permissões de administrador exclusivamente a contas designadas com esse propósito

Limite as permissões de administrador exclusivamente a contas designadas para essa finalidade em todos os ativos empresariais. Realize tarefas comuns de computação, como navegação na Internet, utilização de e-mail e aplicativos de produtividade, a partir da conta de usuário padrão, desprovida de privilégios administrativos. Esta prática visa reforçar a segurança ao minimizar o uso de contas privilegiadas em tarefas cotidianas, reduzindo assim a exposição a riscos potenciais.

4.7. Estabelecer um processo de concessão e revogação de acesso

Estabeleça e adote um procedimento, de preferência automatizado, para conceder acesso aos ativos empresariais em situações de novas contratações, concessão de permissões ou alteração de funções de um usuário. De maneira análoga, institua e siga um procedimento, de preferência automatizado, para retirar o acesso aos ativos empresariais, desativando as contas

imediatamente após o término, revogação de privilégios ou modificação da função de um usuário. A desativação de contas, em detrimento da sua exclusão, pode ser necessária para preservar trilhas de auditoria. Esta prática visa a aprimorar o controle de acessos e a segurança de sistemas e dados corporativos.

4.8 Exigir MFA onde for necessário

Com o objetivo de reforçar a segurança nas operações e estabelecer um controle rigoroso sobre o acesso a recursos de elevada criticidade, é fundamental a adoção da autenticação multifator (MFA) em contextos específicos e estratégicos. Essa prática de segurança é de suma importância e deve ser aplicada em cenários essenciais, abrangendo, entre outros, aplicações expostas externamente, acesso remoto à rede e contas de acesso administrativo. A exigência de MFA nessas circunstâncias é uma medida eficaz para mitigar o risco de acessos não autorizados, proporcionando assim uma camada adicional de proteção para os ativos empresariais e informações confidenciais. A implementação do MFA pode ser simplificada mediante a utilização de serviços de diretório ou soluções de SSO (*Single Sign-On*), que acrescentam robustez e segurança ao processo de autenticação.

Conclusão

Dessa forma, estabelecer uma política de controle de acesso, impondo, por exemplo, o uso de padrões de senhas fortes, procedimentos para exigir mudanças periódicas de senha, e obrigações como não compartilhamento de senhas e não armazenamento de senhas em locais de fácil acesso, pode-se reduzir significativamente o risco de um incidente de segurança cibernética.

Além disso a implementação da autenticação multifator é um passo importante na proteção de sua empresa de telecomunicações contra ameaças cibernéticas. A política de controle de acesso pode ainda, por exemplo, estabelecer várias formas de autenticação, nas quais pode ser adicionada uma camada extra de segurança para ajudar a prevenir o acesso não autorizado a sistemas ou contas críticas. Certifique-se de escolher cuidadosamente uma solução MFA que atenda às necessidades de sua organização e treine os funcionários sobre o uso correto para maximizar sua eficácia.

Capítulo 5: Monitoramento de Atividades e Gestão de Registros de Auditoria

Monitore as atividades em sua rede e sistemas para identificar possíveis ameaças e ataques. Utilize ferramentas de segurança cibernética para automatizar esse processo sempre que possível. Mantenha uma política de gestão de registros de auditoria.

O monitoramento de atividades em sua rede e sistemas é uma das melhores práticas para identificar possíveis ameaças e ataques cibernéticos. Isso permite que você tome medidas proativas para minimizar danos e proteger sua empresa de possíveis violações de segurança. Neste capítulo, discutiremos a importância do monitoramento de atividades e da gestão de registros de auditoria, apresentando sugestões de como implementá-lo em sua prestadora de serviços de telecomunicações.

Como objetivo de tal item pode-se destacar:

Estabelecer e manter uma política de monitoramento de atividades na rede com as ferramentas mais adequadas para o contexto da empresa, bem como estabelecer e manter uma política de gestão de registros(log) de auditoria [3], [4], [5] e [6]

Como modelo inicial para tal processo pode-se utilizar os conceitos, orientações e melhores práticas do Modelo de Política de Gestão de Registros (Logs) de Auditoria do Programa de Privacidade e Segurança da Informação (PPSI) [14].

Por que monitorar atividades?

O monitoramento de atividades em sua rede e sistemas pode ajudar a identificar possíveis ameaças, incluindo tentativas de acesso não autorizado, ataques de *malware* e comportamentos anormais. Por exemplo, o monitoramento de logs pode ajudar a identificar se um usuário está tentando acessar repetidamente uma conta com credenciais inválidas, o que pode ser um sinal de uma tentativa de violação de segurança. É essencial que o monitoramento possua os insumos necessários para possibilitar ações de respostas eficazes em tempo hábil. Além disso, o registro e armazenamento adequado de tais atividades (logs) é essencial para tal monitoramento.

Considere que o monitoramento de atividades pode ajudar a detectar vulnerabilidades em seu sistema e a avaliar a eficácia das medidas de segurança que foram implementadas.

Ferramentas de monitoramento de atividades

Existem várias ferramentas de monitoramento de atividades disponíveis, desde soluções gratuitas até soluções empresariais mais avançadas. Importante avaliar aquelas que melhor podem auxiliar no escopo de atuação da empresa. Algumas das ferramentas comuns incluem:

- Sistema de detecção de intrusão (IDS): monitora o tráfego de rede em busca de atividades suspeitas e maliciosas e emite alertas em caso de violações de segurança.
- Sistema de prevenção de intrusão (IPS): monitora o tráfego de rede e bloqueia atividades suspeitas e maliciosas automaticamente.
- Análise de comportamento do usuário (UBA): monitora o comportamento dos usuários para identificar atividades anormais.
- Sistemas de gerenciamento de informações e eventos de segurança (SIEM): monitoram e analisam logs e alertam os usuários sobre atividades suspeitas.

Como principais medidas para aprimorar o processo de monitoramento, gestão de vulnerabilidades e logs destacam-se:

5.1 Implementar monitoramento de atividades

Para implementar um sistema eficaz de monitoramento de atividades em sua empresa de telecomunicações, é aconselhável começar por uma avaliação das necessidades específicas de monitoramento e pela seleção das ferramentas apropriadas para essa finalidade. A correta implementação das ferramentas é de extrema importância, e é crucial configurá-las para monitorar as atividades relevantes de maneira precisa. Adicionalmente, é essencial estabelecer um procedimento regular de revisão dos registros gerados por essas ferramentas de monitoramento, garantindo que sejam tomadas as medidas adequadas em resposta a quaisquer alertas que possam ser gerados. Este processo assegura a vigilância eficiente das operações da empresa e contribui para a tomada de decisões informadas em relação à segurança e eficácia das telecomunicações.

5.2 Estabelecer e manter um processo de gestão de registros (logs) de auditoria

Institua e preserve um procedimento formal de gestão de registros de auditoria, o qual deve estabelecer os critérios de registro exigidos pela organização. Esse procedimento deve abranger, no mínimo, os aspectos relacionados à coleta, revisão e armazenamento de registros de auditoria referentes aos ativos corporativos. A documentação desse processo deve ser revisada e atualizada anualmente ou sempre que ocorrerem alterações substanciais na empresa que possam afetar

essa prática de segurança. Essa medida assegura o eficaz acompanhamento e registro das atividades críticas, contribuindo para a manutenção da segurança e a conformidade regulatória.

5.3 Coletar registros (logs) de auditoria

Realize a coleta de registros de auditoria de acordo com o procedimento estabelecido para a gestão de logs de auditoria na empresa. Garanta que a ativação do registro tenha sido efetivada em todos os ativos, em conformidade com o mencionado processo de gestão de logs de auditoria. Esta prática é essencial para a obtenção de informações cruciais que sustentam a segurança e a integridade das operações empresariais.

5.4 Garantir o armazenamento adequado dos registros (logs) de auditoria

Assegure que os locais de destino dos registros de auditoria estejam devidamente equipados com capacidade de armazenamento suficiente para atender às exigências do processo de gestão de logs de auditoria da organização. Esta medida é fundamental para garantir a integridade e a disponibilidade dos registros essenciais que sustentam os procedimentos de auditoria e segurança corporativa.

5.5 Assegurar que a infraestrutura de rede esteja atualizada


Garanta que a infraestrutura de rede seja mantida em constante atualização. Isso pode ser alcançado ao manter a última versão estável do software e/ou utilizar soluções de Rede como Serviço (*Network-as-a-Service* - NaaS) que estejam atualmente em suporte. É recomendável realizar revisões das versões do software em intervalos mensais ou mais frequentes, a fim de verificar continuamente o status de suporte das versões utilizadas. Esta prática contribui para a segurança e o desempenho eficiente da infraestrutura de rede da organização.

5.6 Monitorar atividades de terceiros

Realize a monitorização das atividades de fornecedores e parceiros que acessam os sistemas da organização, com o propósito de identificar potenciais ameaças e riscos relacionados à segurança cibernética. Isso engloba a prática regular de supervisão dos registros de acesso, da atividade de rede e da utilização dos recursos dos sistemas. Ao adotar esse procedimento, é possível aprimorar a capacidade de detecção de possíveis ameaças, reforçando a segurança cibernética e a proteção dos sistemas da empresa.

Conclusão

O monitoramento de atividades e a gestão de registro de auditoria são etapas importantes na melhoria da segurança cibernética para prestadoras de serviços de telecomunicações. Ao implementar ferramentas de monitoramento de atividades, você pode identificar ameaças e ataques em seu sistema e tomar medidas proativas para proteger sua empresa de possíveis



violações de segurança. Dessa forma, estabelecer e manter um processo de monitoramento de atividades na rede com as ferramentas mais adequadas para o contexto da empresa, bem como estabelecer e manter uma política de gestão de registros (logs) de auditoria são fatores chaves para garantir a segurança da informação.

Capítulo 6: Backup e Recuperação de Dados

Faça backups regularmente de seus dados críticos e verifique se eles estão funcionando corretamente. Tenha um plano de recuperação para restaurar rapidamente a funcionalidade em caso de falha do sistema.

Os dados são um dos ativos mais valiosos de uma empresa, e protegê-los é fundamental para garantir a continuidade dos negócios em caso de falhas ou ataques cibernéticos. Neste capítulo, discutiremos a importância do backup e da recuperação de dados para prestadoras de telecomunicações.

Como objetivo de tal item pode-se destacar:

Estabelecer e manter um processo de backup e recuperação de dados [3], [4], [5] e [6].

Pode-se utilizar como modelo inicial o documento Modelo de Política de Backup do Programa de Privacidade e Segurança da Informação (PPSI) [15].

Por que criar um processo de backup e recuperação de dados?

Criar um processo de backup e recuperação de dados é fundamental para garantir a continuidade dos negócios e a integridade das informações em caso de falhas de sistema, ataques cibernéticos ou desastres naturais. Backups regulares permitem que uma empresa restaure rapidamente seus dados e sistemas críticos, minimizando o tempo de inatividade e o impacto financeiro. Isso é especialmente importante em um cenário onde as ameaças cibernéticas, como *ransomware*, estão em ascensão [7], e a perda de dados pode não apenas interromper as operações, mas também resultar em perda de reputação e possíveis penalidades legais.

Além disso, um plano de recuperação bem elaborado oferece uma camada extra de segurança ao fornecer um roteiro claro para a restauração de sistemas e dados. Isso é crucial não apenas para responder a eventos imprevistos, mas também para cumprir com regulamentações e padrões da indústria que exigem planos de continuidade de negócios e recuperação de desastres. Ter um processo de backup e recuperação robusto é, portanto, uma prática recomendada que serve como uma apólice de seguro para os ativos digitais de uma empresa.

Como principais medidas para aprimorar o processo de backup e recuperação de dados:

6.1 Estabelecer e manter um processo de recuperação de dados

Institua e mantenha um procedimento formal de recuperação de dados. Nesse processo, aborde de maneira abrangente o âmbito das atividades relacionadas à recuperação de dados, a priorização dessas atividades e a salvaguarda da segurança dos dados de backup. Recomenda-se que a documentação referente a esse processo seja revisada e atualizada anualmente, ou sempre que ocorrerem mudanças substanciais na empresa que possam impactar essa medida de segurança. Esta prática é fundamental para garantir a prontidão e eficácia na recuperação de dados em cenários de incidentes ou desastres, contribuindo para a continuidade das operações e a proteção dos ativos de informação da organização.

6.2 Fazer backup regularmente e automatizado


A realização periódica de cópias de segurança tem como finalidade preservar a integridade e a acessibilidade dos dados, representando uma das medidas mais eficazes para proteger informações críticas em caso de falha do sistema ou de ataques cibernéticos. É crucial que esses backups sejam executados com frequência suficiente para garantir que as informações estejam atualizadas e que os dados mais recentes estejam disponíveis para fins de recuperação. Portanto, é recomendável a implementação de processos automatizados de backup para os ativos corporativos abrangidos por essa política. A frequência dessas operações de cópia de segurança deve ser estabelecida com base na sensibilidade dos dados, sendo realizada semanalmente ou em intervalos mais frequentes, conforme apropriado. Esta abordagem assegura a prontidão e a proteção dos ativos de informação da organização.

6.3 Proteger os dados de recuperação

Com o propósito de prevenir a possibilidade de comprometimento ou de dano aos backups, seja por incidentes cibernéticos ou outros, é fundamental assegurar que os backups não estejam localizados na mesma infraestrutura ou segmento de rede da infraestrutura de produção de onde são coletados. O acesso a esse sistema e segmento de rede deve ser estritamente controlado e submetido a monitoramento constante. Ademais, é imprescindível proteger os dados de recuperação com controles de segurança equivalentes aos aplicados aos dados originais. Isso pode envolver a utilização de criptografia ou a manutenção de uma segregação rigorosa dos dados, dependendo dos requisitos específicos da organização. Essas medidas visam a preservar a integridade e a disponibilidade dos backups, contribuindo para a eficácia do plano de recuperação de dados.

6.4 Estabelecer e manter uma instância isolada de dados de recuperação

Institua e mantenha uma instância separada e independente dos dados de recuperação. Implementações exemplares abarcam a gestão de versões dos destinos de backup através de



sistemas ou serviços que estão fisicamente desconectados do ambiente da empresa, como soluções de armazenamento em nuvem ou repositórios de dados localizados fora das instalações da organização. Esta prática assegura a resiliência e a segurança dos dados de recuperação, reduzindo os riscos de perda ou comprometimento em caso de incidentes.

6.5 Verificar se os backups estão funcionando corretamente

Realizar cópias de segurança dos dados é apenas a etapa inicial. É igualmente crucial realizar verificações regulares para garantir que os backups estejam funcionando adequadamente e que os dados possam ser restaurados com êxito quando necessário. A condução de testes periódicos de restauração é fundamental para identificar eventuais problemas antes que eles alcancem um estágio crítico. Essa prática contribui significativamente para a confiabilidade do processo de backup e a disponibilidade dos dados em cenários de recuperação.

Conclusão

A realização de backups e a capacidade de recuperar dados desempenham um papel fundamental na garantia da integridade e disponibilidade das informações, sendo essenciais para a continuidade dos negócios em situações de falhas ou ataques cibernéticos. Portanto, é imperativo estabelecer e manter um processo de recuperação de dados que englobe a execução regular de cópias de segurança, a adequada proteção desses dados e a realização frequente de verificações para garantir o seu funcionamento adequado. Esta abordagem é crítica para a salvaguarda dos ativos de informação da organização e para a mitigação de riscos associados a incidentes de segurança.

Capítulo 7: Conscientização dos Funcionários sobre Segurança Cibernética

Garanta que seus funcionários estejam cientes dos riscos de segurança cibernética e estejam capacitados para reconhecer e evitar ameaças, bem como preparados para mitigá-las em caso de incidente.

Um dos maiores desafios na segurança cibernética é garantir que todos os funcionários de uma empresa estejam cientes dos riscos e preparados para reconhecer, evitar ameaças e mitigar um incidente [1]. Um único erro humano (acidental ou intencional) pode ser suficiente para permitir que um invasor acesse informações confidenciais, ocasionando graves consequências para a empresa e seus consumidores.

Neste capítulo, vamos discutir a importância da conscientização sobre segurança cibernética para prestadoras de serviços de telecomunicações e como garantir que seus funcionários estejam devidamente treinados para lidar com ameaças cibernéticas e engenharia social.

Como objetivo de tal item pode-se destacar:

Estabelecer e manter um programa de conscientização de segurança cibernética para influenciar o comportamento da força de trabalho, a fim de que tenha consciência dos riscos cibernéticos e esteja devidamente qualificada para reduzir os riscos de segurança cibernética para a empresa. Ações de treinamento teórico e prático são fundamentais em tal programa. [3], [4], [5] e [6].

Materiais de conscientização de referência do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) do Núcleo de Informação e Coordenação do Ponto BR – (NIC.br), hospedados no Portal Internet Segura,⁴ podem ser utilizados para suportar tal programa. Salienta-se que esses materiais de conscientização produzidos pelo NIC.br e disponibilizados no portal estão todos sob licenças *Creative Commons*, permitindo inclusive a

⁴ <https://internetsegura.br/>

impressão com logo da prestadora⁵. O catálogo completo de materiais pode ser consultado no Portal⁶.

Por que a conscientização sobre segurança cibernética é importante para prestadoras de serviços de telecomunicações?

O comportamento humano é crucial para o sucesso da segurança cibernética de uma empresa. Muitas vezes, é mais simples para um invasor enganar um usuário a clicar em um link malicioso do que explorar vulnerabilidades de rede. Usuários podem, mesmo sem intenção, causar incidentes, seja por manuseio inadequado de dados, seja pelo uso de senhas fracas ou repetidas. Cada nível hierárquico na empresa apresenta riscos distintos, com diferentes acessos a dados sensíveis. Para mitigar essas vulnerabilidades humanas, é essencial promover treinamentos constantes, fortalecendo a cultura de segurança e evitando práticas arriscadas.

Uma das principais medidas que as empresas podem tomar é garantir que seus funcionários estejam cientes dos riscos de segurança cibernética e estejam treinados para reconhecer e evitar ameaças. Também é crucial que os funcionários saibam como agir diante de um incidente, adotando as providências necessárias para a sua mitigação. Os funcionários são a primeira linha de defesa contra as ameaças cibernéticas, portanto, é importante que eles estejam preparados para lidar com essas situações.

Como medidas indicadas para auxiliar na conscientização sobre segurança cibernética:

7.1 Estabelecer e manter um programa de conscientização de segurança

A organização deve estabelecer um programa de conscientização em segurança que proporcione educação aos colaboradores sobre as práticas seguras de interação com os ativos e dados corporativos, e permita o cumprimento das principais políticas e diretrizes de segurança cibernética da empresa. O treinamento deve ser ministrado durante o processo de admissão e, no mínimo, anualmente, sendo que o conteúdo deve ser revisado e atualizado anualmente ou sempre que ocorrerem mudanças significativas no ambiente corporativo que possam impactar a segurança. Essa iniciativa é essencial para fortalecer a cultura de segurança na organização e promover a proteção eficaz dos ativos e informações empresariais.

7.2 Conhecer as principais ameaças cibernéticas (ex: engenharia social)

É fundamental promover a conscientização entre os funcionários acerca dos riscos de segurança cibernética mais prevalentes no cenário global, incluindo ameaças como *phishing*, *malware*, ataques de força bruta e engenharia social. É de igual importância que compreendam o

⁵ Verificar informações em: <https://internetsegura.br/licenca/>

⁶ <https://internetsegura.br/pdf/catalogo-internetsegura.pdf>

funcionamento desses ataques a fim de adotar medidas preventivas eficazes. A utilização de exemplos de incidentes cibernéticos passados é uma estratégia válida para ilustrar como tais ameaças poderiam ter sido evitadas, contribuindo assim para uma postura mais proativa na mitigação de riscos de segurança cibernética.

7.3 Conscientização sobre as melhores práticas de autenticação

Promova regularmente sessões de treinamento destinadas aos funcionários abordando as melhores práticas relacionadas à autenticação. Exemplificando, os tópicos podem incluir a autenticação multifator (MFA), a criação de senhas seguras e a eficaz gestão de credenciais. Essas ações visam capacitar os envolvidos a adotar medidas de segurança robustas durante o processo de autenticação, contribuindo para a proteção dos sistemas e dados.

7.4 Treinar membros da força de trabalho sobre as causas da exposição não intencional de dados

Instrua os integrantes da equipe para que compreendam as razões por trás da exposição não intencional de dados. Tópicos de interesse podem abordar situações como a entrega inadequada de informações sensíveis, a perda de dispositivos móveis ou a divulgação de dados a públicos não autorizados. Essa capacitação visa sensibilizar os colaboradores sobre os potenciais cenários de exposição de dados e a importância de evitar tais situações, contribuindo assim para a proteção das informações corporativas e proteção dos dados pessoais dos consumidores da empresa.

7.5 Conscientizar sobre o plano de resposta a incidentes

Capacite os colaboradores para identificar potenciais incidentes e comunicá-los adequadamente. Apesar de todos os investimentos em segurança, é imprescindível reconhecer que incidentes cibernéticos podem ocorrer. Nesse contexto, é crucial implementar um plano de resposta a incidentes que detalhe as ações a serem tomadas diante de ataques cibernéticos, garantindo que todos os funcionários estejam cientes de suas responsabilidades em tais circunstâncias.

7.6 Treinar a força de trabalho sobre como identificar e comunicar se os seus ativos corporativos não estão atualizados corretamente

Instrua os membros da equipe a adquirir competências para identificar e reportar adequadamente problemas relacionados às atualizações de software, bem como quaisquer disfunções em ferramentas e processos automatizados. Essa capacitação deve incorporar, como parte fundamental, o procedimento de informar a equipe de Tecnologia da Informação (TI) acerca de quaisquer irregularidades em tais processos.

7.7 Treinar a força de trabalho sobre os riscos de se conectar e transmitir dados corporativos em redes inseguras

Capacite os colaboradores sobre os riscos associados à conexão e à transmissão de dados em redes não seguras para fins corporativos. No caso de a empresa contar com funcionários em trabalho remoto, o treinamento deve abranger diretrizes que assegurem que todos os usuários configurem adequadamente a infraestrutura de rede em seus ambientes domésticos, garantindo a segurança das comunicações e dos dados corporativos.

7.8 Conscientizar sobre as fragilidades críticas em equipamentos instalados

Realizar monitoramento para identificar possíveis vulnerabilidades críticas nos dispositivos utilizados pela empresa, incluindo aqueles instalados nos sistemas dos consumidores, que possam representar uma ameaça à segurança e à privacidade.

7.9 Fornecer treinamento em segurança cibernética para terceiros

Ofereça programas de treinamento em segurança cibernética aos fornecedores e parceiros que acessam seus sistemas. Essa iniciativa visa assegurar que essas partes tenham uma compreensão sólida das melhores práticas de segurança cibernética, contribuindo para a redução dos riscos de violações de segurança.

Conclusão

A conscientização sobre segurança cibernética é essencial para ampliar a proteção das prestadoras de serviços de telecomunicações diante de ataques cibernéticos. É fundamental que os funcionários estejam cientes dos riscos de segurança cibernética e saibam como identificar e evitar ameaças. Além disso, a criação do programa de conscientização de segurança cibernética e o treinamento regular dos funcionários são fundamentais para a prevenção de incidentes cibernéticos e para a proteção dos dados da empresa e de seus consumidores.

Capítulo 8: Conscientização dos Consumidores sobre Segurança Cibernética

Promova ações para que seus consumidores fiquem cientes dos riscos de segurança cibernética e tenham condições de reconhecer e evitar ameaças.

Um dos maiores desafios na segurança cibernética é garantir que todas as pessoas que utilizam as Tecnologias de Informação e Comunicação (TICs), como a Internet por exemplo, estejam cientes dos riscos e preparados para reconhecer, evitar ameaças e mitigar um incidente [1]. Um único erro humano pode ser suficiente para permitir que um invasor acesse informações confidenciais, ocasionando graves consequências para a vítima. De forma semelhante, pode viabilizar que a rede e dispositivos da vítima possam ser utilizados para ataques cibernéticos, dando poder de fogo aos atacantes para a realização de Ataques Distribuídos de Negação de Serviço (DDoS), por exemplo.

Neste capítulo, vamos discutir a importância da conscientização sobre segurança cibernética dos consumidores das prestadoras de serviços de telecomunicações e como promover iniciativas para a sua conscientização.

Como objetivo do item pode-se destacar:

Estabelecer e manter um programa de conscientização de segurança cibernética para os consumidores, para que tenham ciência e possam se proteger dos riscos e ameaças cibernéticas, também contribuindo para a segurança das redes de telecomunicações. Campanhas de conscientização são fundamentais em tal programa.

Materiais de conscientização de referência do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) do Núcleo de Informação e Coordenação do Ponto BR – (NIC.br), hospedados no Portal Internet Segura,⁷ podem ser utilizados para suportar esse programa. Salienta-se que esses materiais de conscientização produzidos pelo NIC.br e disponibilizados no portal estão todos sob licenças *Creative Commons*, permitindo inclusive a impressão com logo da prestadora⁸. O catálogo completo de materiais pode ser consultado no

⁷ <https://internetsegura.br/>

⁸ Verificar informações em: <https://internetsegura.br/licenca/>

Portal⁹. Ademais, destaca-se ainda a existência do Movimento #FiqueEsperto, uma iniciativa de assinatura coletiva que abrange a Agência e o setor de telecomunicações¹⁰, cujos materiais de campanha e mensagens podem ser utilizados para a conscientização principalmente dos consumidores.

Por que a conscientização sobre segurança cibernética dos consumidores é importante para prestadoras de serviços de telecomunicações?

O comportamento humano é crucial para a segurança cibernética e o comportamento de cada consumidor pode impactar na segurança da rede da prestadora, visto que a sua rede doméstica e seus dispositivos podem ser utilizados para tentativas de invasão da rede da prestadora e ataques de massa. Assim, fomentar um comportamento mais seguro do consumidor contribui para a segurança cibernética do ecossistema digital como um todo, podendo inclusive se tornar um diferencial competitivo para a empresa, uma vez que essas práticas comerciais abrangem medidas de cuidado para com o seu consumidor.

Além disso, um comportamento mais seguro do consumidor reduz a sua exposição aos riscos do ambiente digital, fazendo com que o consumidor se sinta confiante na utilização das TICs e prevenindo a ocorrência de incidentes cibernéticos, bem como contribuindo para que o consumidor não seja vítima de fraudes no ambiente digital.

Como medidas indicadas para auxiliar na conscientização sobre segurança cibernética:

8.1 Estabelecer e manter um programa de conscientização de segurança

A organização deve estabelecer um programa de conscientização em segurança cibernética focada no consumidor que proporcione a sua educação sobre os riscos e sobre as práticas seguras de utilização das TICs. As ações precisam ser desenvolvidas de maneira continuada e perene. Essa iniciativa é essencial para promover a cultura de segurança cibernética que precisa contemplar todos os atores do ecossistema.

8.2 Explorar diferentes materiais e abordagens, reconhecendo as diferenças e as necessidades de diversos grupos sociais

As ações de conscientização dos consumidores podem e devem explorar diferentes abordagens e materiais, também reconhecendo a diversidade e a necessidade dos diferentes grupos sociais, como, por exemplo, crianças, adolescentes e idosos. Datas temáticas como o Dia da Internet Segura (celebrado sempre no início de fevereiro todos os anos); Dia Internacional do Idoso (1º de

⁹ <https://internetsegura.br/pdf/catalogo-internetsegura.pdf>

¹⁰ <https://fe.seg.br/>

outubro); e Dia das Crianças (12 de outubro) podem ser utilizadas para sensibilizar os consumidores.

8.3 Conhecer as principais ameaças cibernéticas (ex: engenharia social)

É fundamental que as ações de promoção de conscientização abarquem o alerta dos consumidores acerca dos riscos de segurança cibernética mais frequentes, incluindo ameaças como *phishing*, *malware*, ataques de força bruta e engenharia social. É de igual importância que compreendam o funcionamento desses ataques a fim de poderem reconhecê-los, evitá-los e adotar medidas preventivas eficazes.

8.4 Conscientização sobre as melhores práticas de autenticação

Um dos tópicos que deve ser regularmente abordado nas medidas adotadas refere-se às melhores práticas relacionadas à autenticação, incluindo a autenticação multifator (MFA) e a criação de senhas seguras para a rede doméstica do consumidor, seus dispositivos e suas aplicações, como uma prática basilar de um comportamento seguro.

8.5 Educar os consumidores sobre os riscos de se conectar e transmitir dados em redes inseguras

Consumidores devem ser alertados quanto aos riscos associados à conexão e à transmissão de dados em redes não seguras, as quais podem apresentar riscos elevados para os seus dados, especialmente para determinadas aplicações, como por exemplo, a utilização de aplicativos de instituições financeiras para realização de transações.

Conclusão

A conscientização sobre segurança cibernética é essencial para a segurança dos consumidores, da sua rede doméstica, dos seus dispositivos e dos seus dados. Não obstante, a adoção de um comportamento cibernético mais seguro pelos consumidores também contribui para a segurança das redes da sua prestadora de serviço de telecomunicações, bem como das demais redes e para todo o ecossistema digital.

Capítulo 9: Segurança Física

Proteja seus sistemas e dados com medidas físicas de segurança, como controle de acesso físico e monitoramento com câmeras, e adote uma política de mesa limpa e tela limpa.

Além das medidas de segurança digital, a segurança física também é crucial para proteger sua empresa de telecomunicações contra ameaças cibernéticas. Neste capítulo, discutiremos algumas práticas recomendadas para garantir a segurança física dos seus sistemas e dados.

Como objetivo de tal item pode-se destacar:

Estabelecer e manter uma política de segurança física para sistemas e dados [3], [4], [5] e [6].

Por que o processo de segurança física é importante para proteger sistemas e dados contra ameaças cibernéticas?

O processo de segurança física é uma componente essencial da estratégia global de segurança de uma organização, pois aborda as ameaças que podem surgir no ambiente físico no qual os sistemas e dados estão armazenados e operados. Embora as ameaças cibernéticas sejam frequentemente associadas a ataques virtuais, como *malware* ou *phishing*, a verdade é que muitos incidentes de segurança podem ser iniciados ou facilitados por meio de acesso físico não autorizado. Dessa forma, importante estabelecer proteção da área que contenham informações e outros ativos associados, como por exemplo 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 possa ocorrer facilmente).

Como medidas básicas indicadas para auxiliar no processo de segurança física destacam-se:

9.1 Estabelecer controle de acesso físico

O controle de acesso representa uma das medidas de segurança física de maior importância que sua empresa pode adotar. Isso engloba a restrição do acesso às áreas onde sistemas e dados são armazenados, além da implementação de um sistema de autenticação seguro que permita o acesso somente a indivíduos autorizados. A implementação de controles, tais como cartões de acesso, biometria ou a presença de guardas de segurança, visa a garantir que somente pessoas autorizadas tenham permissão para entrar em áreas restritas. Ademais, é crucial assegurar que

locais específicos, como salas de servidores, apresentem camadas adicionais de segurança, como fechaduras reforçadas ou sistemas de alarme.

9.2 Estabelecer monitoramento por câmeras

A implementação de sistemas de vigilância por câmeras representa um método eficaz para a supervisão das operações em sua empresa. É imperativo que as câmeras sejam estrategicamente posicionadas em locais críticos, como as salas de servidores, a fim de monitorar e registrar quaisquer atividades suspeitas. Além disso, é crucial que as gravações sejam armazenadas em um local seguro e que o acesso a esses registros seja concedido apenas a indivíduos autorizados.

9.3 Proteger equipamentos

Os ativos físicos da empresa também requerem medidas de proteção abrangentes para mitigar riscos, como danos, furto ou acesso não autorizado. É vital que instalações que abriguem servidores ou outros equipamentos críticos sejam estrategicamente posicionadas, distantes de áreas de alto tráfego, a fim de reduzir acessos desnecessários. Além disso, essas instalações devem ser protegidas de maneira a prevenir perdas, danos, roubo, incêndio, exposição a explosivos, à fumaça, à poeira e à água, variações de temperatura e qualquer forma de comprometimento de ativos que possa interromper as operações da organização. Nessas instalações, é fundamental proibir rigorosamente o consumo de alimentos, bebidas, tabaco ou qualquer outra substância que possa resultar em resíduos sólidos, líquidos ou gasosos. Além disso, é recomendável avaliar a implementação de controles de acesso no nível da porta, como o protocolo 802.1x ou protocolos similares de controle de acesso à rede, que possam incluir autenticação de usuário e/ou dispositivo para fortalecer ainda mais a segurança.

9.4 Política de mesa limpa e tela limpa

Essa política tem como objetivo primordial mitigar os riscos associados ao acesso não autorizado, à perda e aos danos de informações que podem estar expostas em mesas, telas e outros locais de fácil acesso, tanto durante o horário comercial, quanto fora dele. Para alcançar tal objetivo, as organizações devem estabelecer e comunicar de maneira clara uma política específica que englobe diretrizes como:

- **Armazenamento de Informações Sensíveis ou Críticas:** deve ser prática padrão guardar informações sensíveis ou críticas em locais seguros quando não estiverem sendo utilizadas;
- **Proteção de Dispositivos:** todos os dispositivos devem ser protegidos com mecanismos de segurança adequados para evitar acesso não autorizado;

- Configuração de Computadores: configurar os computadores para realizar o desligamento ou logout automático após um período definido de inatividade, reduzindo assim os riscos associados à exposição de informações confidenciais;
- Gerenciamento de Impressões: impressões devem ser coletadas imediatamente e armazenadas de forma segura para evitar que informações sensíveis fiquem expostas;
- Configuração de *Pop-ups*: é fundamental estabelecer regras para a configuração de pop-ups em telas, incluindo a desativação de notificações de e-mail e mensagens durante apresentações ou atividades semelhantes; e
- Limpeza de *Displays*: informações sensíveis ou críticas exibidas em quadros brancos e outros *displays* devem ser apagadas prontamente quando não forem mais necessárias.

Conclusão

A segurança física também é parte da estratégia de segurança cibernética de sua empresa de telecomunicações. Ao implementar medidas como controle de acesso, monitoramento por câmeras, criação de uma política de mesa limpa e tela limpa, proteção de equipamentos e cabeamento pode-se ampliar a segurança dos seus sistemas e dados.

Capítulo 10: Plano de Resposta a Incidentes

Tenha um plano de resposta a incidentes em vigor para minimizar danos em caso de violação de segurança.

Apesar de todas as medidas preventivas de segurança cibernética, é importante ter um plano de resposta a incidentes em vigor para lidar com possíveis violações de segurança. Um plano de resposta a incidentes ajuda a minimizar danos e tempo de inatividade, além de permitir uma resposta rápida, organizada e eficaz ao incidente.

Como objetivo do item pode-se destacar:

Estabelecer um plano de resposta a incidentes para desenvolver e manter uma capacidade de resposta a incidentes (por exemplo, políticas, planos, procedimentos, funções definidas, treinamento e comunicações) para preparar, detectar e responder rapidamente a um ataque de acordo com o escopo e necessidade da organização. [3], [4], [5] e [6].

Como modelo inicial para tal plano pode-se utilizar o Guia de Resposta a Incidentes do Programa de Privacidade e Segurança da Informação (PPSI) [16].

Por que criar um plano de resposta a incidentes?

A resposta a incidentes tem como objetivo identificar ameaças, intervir antes de sua propagação e remediar questões antes que resultem em danos. Sem um entendimento integral do incidente, as organizações podem permanecer em um ciclo contínuo de resposta, sem a capacidade de aprimorar suas defesas.

Adicionalmente, não é realista presumir que as medidas de proteção sejam infalíveis. Na ocorrência de um incidente, na ausência de um plano documentado, as organizações enfrentam desafios para adotar os procedimentos adequados de investigação, elaboração de relatórios e comunicação. A comunicação eficaz com as partes interessadas é de suma importância. A gestão organizacional deve estar informada sobre os impactos potenciais a fim de tomar decisões fundamentadas sobre remediação, considerando aspectos como conformidade regulamentar, acordos com terceiros e impactos financeiros ou operacionais potenciais.

Como medidas básicas indicadas para auxiliar na criação do plano de resposta a incidentes destacam-se:

10.1 Designar pessoal para gerenciar tratamento de incidentes

Nomeie um responsável e, no mínimo, um substituto para liderar o processo de tratamento de incidentes da empresa. A equipe de gestão é encarregada de coordenar e documentar os esforços relacionados à resposta e recuperação de incidentes, e pode ser composta por membros da equipe interna da organização, fornecedores terceirizados ou adotar uma abordagem híbrida que combine ambos. Caso a empresa opte por envolver fornecedores terceirizados, é fundamental designar, pelo menos, um membro da equipe interna para supervisionar e garantir a eficácia das atividades terceirizadas. Esta designação deve ser revisada anualmente ou sempre que ocorrerem mudanças significativas na empresa que possam impactar a capacidade de resposta a incidentes e a segurança geral da organização.

10.2 Estabelecer e manter informações de contato para relatar incidentes de segurança

Defina e mantenha registros das informações de contato das partes que devem ser notificadas em caso de incidentes de segurança. Esses contatos podem abranger funcionários internos, parceiros de fornecimento terceirizado, autoridades policiais, fornecedores de seguros cibernéticos, agências governamentais pertinentes e outras partes interessadas relevantes. Realize uma revisão anual dos detalhes de contato para assegurar que estejam atualizados e prontos para serem acionados em emergências ou incidentes de segurança.

10.3 Estabelecer e manter um processo corporativo para relatar incidentes

Institua e mantenha um procedimento empresarial destinado à comunicação de incidentes de segurança pela força de trabalho. Este procedimento deve abranger os prazos para notificação, o pessoal responsável por efetuar os relatórios, os mecanismos utilizados para comunicar tais incidentes e os dados mínimos requeridos nos relatórios. Assegure-se de que este processo esteja prontamente acessível a todos os membros da força de trabalho. Faça uma revisão anual do procedimento ou sempre que ocorrerem mudanças substanciais na empresa que possam influenciar este controle de segurança.

Conclusão

A elaboração e implementação de um plano de resposta a incidentes é de importância fundamental na mitigação dos prejuízos decorrentes de uma violação de segurança. Um plano claramente definido, que seja objeto de treinamento periódico, desempenha um papel significativo na redução do tempo de inatividade e no minimizar do impacto causado por tais incidentes.

Capítulo 11: Política de Segurança Cibernética

Tenha uma Política de Segurança Cibernética aprovada pela alta gestão, publicada e comunicada aos colaboradores e às partes interessadas, e revisada em intervalos planejados e quando ocorrerem alterações significativas.

A segurança cibernética é um pilar fundamental para qualquer organização, especialmente para prestadoras de serviços de telecomunicações que possuem uma grande superfície de ataque em razão da atividade econômica que exploram, com redes, equipamentos, e tratamento de uma vasta quantidade de dados, incluindo dados pessoais. A Política de Segurança Cibernética é um conjunto de princípios que norteia a gestão de segurança cibernética e que deve ser observado pelo corpo técnico e gerencial, bem como pelos usuários internos e externos. As diretrizes estabelecidas nesta política determinam as linhas mestras que devem ser seguidas pela instituição para que sejam asseguradas suas redes, seus recursos computacionais e suas informações. Tais diretrizes e práticas visam proteger a informação contra ameaças, garantindo sua confidencialidade, integridade e disponibilidade.

Neste capítulo, abordaremos os controles básicos das melhores práticas para a Política de Segurança Cibernética, destacando sua importância e como implementá-los efetivamente.

Como objetivo de desse tópico pode-se destacar:

Estabelecer e manter uma Política de Segurança Cibernética [2], [3], [4], [5], [6] e [18].

Como inspiração inicial para tal política pode-se utilizar os conceitos, orientações e melhores práticas do Guia para o desenvolvimento de uma Política de Segurança da Informação e Comunicação da Rede Nacional de Ensino e Pesquisa (RNP) [18].

Cabe esclarecer que segurança da informação é um campo mais amplo, abrangendo segurança cibernética; defesa cibernética; segurança física e proteção de dados organizacionais; e ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação, nos termos da Política Nacional de Segurança da Informação [19]. Assim, a política elaborada, mantida e implementada pelas prestadoras pode também ser mais ampla, abarcando outros tópicos de segurança da informação ou relacionados, como privacidade e proteção de dados.

Por que uma Política de Segurança Cibernética é essencial para prestadoras de serviços de telecomunicações?

As prestadoras de serviços de telecomunicações são alvos frequentes de ataques cibernéticos devido à natureza valiosa das informações que possuem e da essencialidade dos serviços que prestam. Uma política robusta de segurança cibernética não apenas protege a organização contra ameaças externas, mas também define padrões e comportamentos seguros para os funcionários, minimizando riscos internos. Ela também considera a estratégia e requisitos de negócios, os regulamentos, legislação e contratos, bem como os riscos e ameaças de segurança cibernética atuais e projetados. Dessa forma, consegue estar alinhada às principais diretrizes da empresa e em conformidade com as principais determinações legais e técnicas, bem como com as melhores práticas.

Como medidas básicas para serem consideradas na Política de Segurança Cibernética destacam-se:

11.1 Definir segurança cibernética

Estabelecer e documentar uma definição clara e compreensível de segurança cibernética que seja relevante para a organização.

11.2 Estabelecer objetivos e princípios de segurança cibernética

Definir e documentar os objetivos específicos e princípios fundamentais da segurança cibernética que orientarão todas as atividades e decisões relacionadas à segurança cibernética na organização. Criar um quadro estruturado para a definição e revisão regular destes objetivos.

11.3 Estabelecer diretrizes e requisitos de segurança cibernética

Garantir que a organização esteja comprometida em satisfazer todos os requisitos legais, regulamentares e contratuais aplicáveis relacionados à segurança cibernética. Assim devem ser apresentadas as diretrizes e requisitos para a proteção da organização (redes, sistemas e dados) e para que a segurança seja estabelecida e cumpra seu papel.

11.4 Atribuir responsabilidades relacionadas à segurança cibernética

Definir e documentar as responsabilidades específicas relacionadas à gestão de segurança cibernética. Atribuir estas responsabilidades a funções ou cargos específicos dentro da organização, garantindo que haja clareza sobre quem é responsável por quais aspectos de segurança cibernética.

11.5 Definir as sanções disciplinares

A política de segurança cibernética deve estabelecer sanções disciplinares para descumprimento de suas diretrizes, alinhadas às normas e contratos da organização. Um processo aprovado pela gestão deve ser implementado para tratar tais descumprimentos. Além disso, é aconselhável que os funcionários assinem um Termo de Responsabilidade, confirmando seu entendimento e compromisso com a política e reconhecendo as possíveis penalidades por infrações.

Conclusão

A Política de Segurança Cibernética é mais do que um conjunto de diretrizes; é uma estratégia abrangente que protege os ativos mais valiosos de uma organização. Além disso todas as demais políticas indicadas no presente guia devem suportar e auxiliar tal política na implementação de controles de segurança cibernética. Estas políticas específicas devem ser alinhadas e complementares à Política de Segurança Cibernética da organização. Para prestadoras de telecomunicações, a implementação e manutenção rigorosa desta política são essenciais para garantir a confiança dos consumidores, a integridade, confidencialidade e disponibilidade dos dados e a continuidade dos negócios.

Considerações Finais

A era digital trouxe consigo uma série de benefícios e oportunidades para as empresas, especialmente para as prestadoras de telecomunicações. No entanto, com essas oportunidades, surgem também desafios significativos, principalmente no que diz respeito à segurança cibernética e à proteção de dados. O presente guia buscou abordar, de maneira estruturada e detalhada, as melhores práticas e diretrizes para garantir um ambiente digital seguro e confiável.


Ao longo dos capítulos, discutimos desde a importância do inventário de ativos até a elaboração de políticas robustas de segurança da informação. Cada capítulo foi projetado para fornecer às prestadoras de serviços de telecomunicações as ferramentas e conhecimentos necessários, **em nível básico**, para enfrentar as ameaças cibernéticas contemporâneas. O Guia não deve ser compreendido como um ponto de chegada, mas um ponto de partida para auxiliar as prestadoras nessa jornada. E considerando que traz as capacidades básicas que precisam ser construídas, implementadas e mantidas, tem utilidade especial às Prestadoras de Pequeno Porte no setor.

A segurança cibernética não é uma tarefa única ou um objetivo final, mas sim um processo contínuo. As ameaças evoluem, assim como as tecnologias e as práticas recomendadas. Portanto, é imperativo que as empresas estejam sempre atualizadas, revisando e adaptando suas estratégias de segurança conforme necessário.

A adoção das práticas recomendadas neste guia não apenas fortalecerá a segurança das redes e sistemas das prestadoras de telecomunicações, mas também reforçará a confiança de seus consumidores e parceiros. A segurança cibernética é, em última análise, uma responsabilidade compartilhada, e todos os envolvidos – desde os técnicos de TI até a alta administração – devem estar comprometidos com sua implementação e manutenção.

Por fim, é importante ressaltar que, embora este guia forneça uma base sólida para a segurança cibernética, ele deve ser complementado com treinamento contínuo, conscientização e avaliações periódicas de risco. Apenas através de uma abordagem holística e integrada, as prestadoras de serviços de telecomunicações poderão enfrentar eficazmente os desafios da segurança cibernética e garantir um futuro digital seguro para todos.

Agradecemos a todos os colaboradores e especialistas que contribuíram para a elaboração do guia e esperamos que ele sirva como um recurso valioso para as prestadoras de serviços de telecomunicações em sua jornada contínua de segurança e resiliência cibernéticas.



Como instrumento prático e de alto nível foi elaborado um *checklist* de melhores práticas de nível básico de segurança cibernética para prestadoras de serviços de telecomunicações para uma autoavaliação rápida que seja útil para nortear possíveis ações e investimentos sobre os temas discutidos neste guia.



Checklist de Segurança Cibernética para Prestadoras de Serviços de Telecomunicações Nível Básico



Consulte mais informações no guia completo em www.bit.ly/guiaciber2023

- ☐ **Inventário de Ativos:** Gerenciar constantemente os ativos institucionais e softwares, com o objetivo de identificar precisamente quais necessitam ser monitorados, bloqueados e/ou protegidos dentro da empresa.
- ☐ **Proteção de Dados:** Desenvolva processos e controles técnicos para identificar, classificar, manusear com segurança, reter e descartar dados.
- ☐ **Configuração Segura de Ativos:** Defina e mantenha a configuração segura de recursos empresariais (ex: dispositivos móveis; equipamentos e servidores; e programas (ex:sistemas e aplicações).
- ☐ **Controle de Acesso e Contas:** Use processos e ferramentas para atribuir e gerenciar autorização de credenciais, bem como criar, atribuir, gerenciar e revogar credenciais de acesso e privilégios para contas (ex: usuário e admin.)
- ☐ **Monitoramento de Atividades e Gestão de Vulnerabilidades e Registros:** Monitore as atividades em sua rede e sistemas para identificar possíveis ameaças e ataques, de forma automatizada, sempre que possível. Mantenha um processo de gestão de vulnerabilidades e de registros de auditoria.
- ☐ **Backup e Recuperação de Dados:** Faça backups regularmente de seus dados críticos e verifique se eles estão funcionando corretamente. Tenha um plano de recuperação para restaurar a funcionalidade em caso de falha do sistema.
- ☐ **Conscientização de Segurança Cibernética para os Funcionários:** Garanta que seus funcionários estejam cientes dos riscos de segurança cibernética e estejam treinados para reconhecer e evitar ameaças.
- ☐ **Conscientização de Segurança Cibernética para os Consumidores:** Fomente um comportamento mais seguro dos seus consumidores para reconhecer e evitar ameaças cibernéticas.
- ☐ **Segurança Física:** Proteja seus sistemas e dados com medidas físicas de segurança, como controle de acesso físico, monitoramento com câmeras e adote uma política de mesa limpa e tela limpa.
- ☐ **Plano de Resposta a Incidentes:** Tenha um plano de resposta a incidentes em vigor para minimizar danos em caso de violação de segurança
- ☐ **Política de Segurança da Cibernética:** Tenha uma política aprovada pela alta gestão, publicadas e comunicadas aos colaboradores relevantes, para nortear a gestão de segurança cibernética na prestadora.

Lembre-se: as ações para aprimorar a segurança cibernética devem ser contínuas. Atualize e aprimore-as regularmente para garantir a proteção da sua prestadora de telecomunicações!

Referências

- [1] SONICWALL, 2023 Cyber Threat Report, Charting Cybercrime's shifting frontlines. Disponível em: <https://www.sonicwall.com/2023-cyber-threat-report/>. Acesso em: 14 ago. 2023.
- [2] BRASIL. Agência Nacional de Telecomunicações. Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações, aprovado pela Resolução nº 740, de 21 de dezembro de 2020. Disponível em: <https://informacoes.anatel.gov.br/legislacao/index.php/component/content/article?id=1497>. Acesso em 24 ago. 2023.
- [3] CENTER INTERNET SECURITY. Controles CIS Versão 8. Disponível em: <https://www.cisecurity.org/controls/v8>. Acesso em: 8 ago. 2023.
- [4] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Guia de Aperfeiçoamento da Segurança Cibernética para Infraestrutura Crítica, versão 1.1, 2018. Disponível em: <https://www.nist.gov/cyberframework/framework>. Acesso em: 9 ago. 2023.
- [5] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27001:2022: Segurança da informação, segurança cibernética e proteção à privacidade – Sistemas de gestão da segurança da informação – Requisitos. Rio de Janeiro, 2022.
- [6] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27002:2022– Tecnologia da Informação – Técnicas de Segurança – Código de Prática para Controles de Segurança da Informação. Rio de Janeiro, 2022.
- [7] BRASIL. Presidência da República. Ministério da Economia. Secretaria de Governo Digital, Portaria SGD/MGI nº 852, de 28 de março de 2023, que dispõe sobre o Programa de Privacidade e Segurança da Informação – PPSI. Disponível em: <https://www.in.gov.br/en/web/dou/-/portaria-sgd/mgi-n-852-de-28-de-marco-de-2023-473750908>. Acesso em: 14 ago. 2023.
- [8] BRASIL. Presidência da República. Gabinete de Segurança Institucional. Portaria nº 93, de 26 de setembro de 2019. Glossário de Segurança da Informação. Disponível em: <https://www.in.gov.br/en/web/dou/-/portaria-n-93-de-26-de-setembro-de-2019-219115663>. Acesso em: 16 ago. 2023.
- [9] BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). Guia Orientativo sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf>. Acesso em: 20 set. 2023.

[10] THE CYBERTHREAT REPORT, June 2023. Insights Gleaned from a Global Network of Experts, Sensors, Telemetry, and Intelligence. Disponível em: <https://www.trellix.com/en-us/advanced-research-center/threat-reports/jun-2023.html> Acesso em: 4 ago. 2023.

[11] BRASIL. Presidência da República. Ministério da Economia. Secretaria de Governo Digital. Modelo de Política de Gestão de Ativos, Programa de Privacidade e Segurança da Informação – PPSI. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/modelo_politica_gestao_ativos.pdf. Acesso em: 16 ago. 2023.

[12] BRASIL. Presidência da República. Ministério da Economia. Secretaria de Governo Digital. Guia de Gerenciamento de Vulnerabilidades, Programa de Privacidade e Segurança da Informação – PPSI. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_gerenciamento_vulnerabilidades.pdf. Acesso em: 16 ago. 2023.

[13] BRASIL. Presidência da República. Ministério da Economia. Secretaria de Governo Digital. Modelo de Política de Gestão de Controle de Acesso, Programa de Privacidade e Segurança da Informação – PPSI. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/modelo_politica_controle_acesso.pdf. Acesso em: 16 ago. 2023.

[14] BRASIL. Presidência da República. Ministério da Economia. Secretaria de Governo Digital. Modelo de Política de Gestão de Registros (Logs) de Auditoria, Programa de Privacidade e Segurança da Informação – PPSI. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/modelo_politica_logs_auditoria.pdf. Acesso em: 16 ago. 2023.

[15] BRASIL. Presidência da República. Ministério da Economia. Secretaria de Governo Digital. Modelo de Política de Backup, Programa de Privacidade e Segurança da Informação – PPSI. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/modelo_politica_backup.pdf. Acesso em: 22 ago., 2023.

[16] BRASIL. Presidência da República. Ministério da Economia. Secretaria de Governo Digital. Guia de Resposta a Incidentes de Segurança, Programa de Privacidade e Segurança da Informação – PPSI. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_resposta_incidentes.pdf. Acesso: 22 ago. 2023.

[17] ENISA, European Union Agency for Cybersecurity, 5G Security Controls Matrix - ENISA - European Union, 2023. Disponível em: <https://www.enisa.europa.eu/publications/5g-security-controls-matrix> Acesso em 31 ago. 2023

[18] RNP. Rede Nacional de Ensino e Pesquisa. Guia para Desenvolvimento de uma Política de Segurança da Informação e Comunicação, 2016. Disponível em:

https://www.rnp.br/arquivos/guia_para_desenvolvimento_de_uma_posic-v1.0.docx. Acesso em: 31 ago. 2023.

[19] BRASIL. Decreto nº 9.637, de 26 de dezembro de 2018, que institui Política Nacional de Segurança da Informação. Disponível em: http://www.planalto.gov.br/ccivil_03/ato2015-2018/2018/decreto/D9637.htm. Acesso em: 21 set. 2023.

[20] CERT.BR, Cartilha PHISHING E OUTROS GOLPES, 2022, Disponível em: <https://cartilha.cert.br/fasciculos/phishing-golpes/fasciculo-phishing-golpes.pdf>. Acesso em 31 ago. 2023

Glossário

- **Ambiente/Espaço Cibernético:** espaço virtual composto por um conjunto de canais de comunicação da internet e outras redes de comunicação que garantem a interconexão de dispositivos de TIC e que engloba todas as formas de atividades digitais em rede, incluindo o armazenamento, processamento e compartilhamento de conteúdo além de todas as ações, humanas ou automatizadas, conduzidas através desse ambiente.[2]
- **Ambiente em nuvem:** Um ambiente virtualizado que fornece acesso conveniente à rede sob demanda a um pool compartilhado de recursos configuráveis, como rede, computação, armazenamento, aplicações e serviços. Existem cinco características essenciais para um ambiente de nuvem: autoatendimento sob demanda, amplo acesso à rede, pool de recursos, elasticidade rápida e serviço medido. Alguns serviços oferecidos por meio de ambientes de nuvem incluem *Software as a Service* (SaaS), *Platform as a Service* (PaaS) e *Infrastructure as a Service* (IaaS).[3]
- **Ambiente físico:** Componentes físicos de hardware que constituem uma rede, incluindo cabos e roteadores. O hardware é necessário para comunicação e interação entre dispositivos em uma rede.[3]
- **Ambiente virtual:** Simulação de hardware que permite que um ambiente de software seja executado sem a necessidade de usar hardware real. Ambientes virtualizados são usados para fazer com que um pequeno número de recursos atue como muitos, com bastante processamento, memória, armazenamento e capacidade de rede. A virtualização é uma tecnologia fundamental que permite que a computação em nuvem funcione.[3]
- **Ameaça:** conjunto de fatores externos com o potencial de causar em dano para um sistema ou organização.[8]
- **Aplicação:** Um programa, ou grupo de programas, hospedado em ativos corporativos e projetado para usuários finais. As aplicações são consideradas um ativo de software neste documento. Os exemplos incluem aplicações web, de banco de dados, baseadas em nuvem e móveis.[3]
- **Acesso:** Permissão para entrar em um sistema, rede ou aplicativo.[3]
- **Ameaças Cibernéticas:** Ataques potenciais ou tentativas de exploração de sistemas, redes ou informações.[3]
- **ATIVO** - tudo que tenha valor para a organização, material ou não.[8]
- **Ativos corporativos:** Ativos com potencial para armazenar ou processar dados. Para os fins deste documento, os ativos corporativos incluem dispositivos de usuário final,

dispositivos de rede, dispositivos não computacionais/Internet das Coisas (IoT) e servidores em ambientes virtuais, baseados em nuvem e físicos.[3]

- **Ativos corporativos expostos externamente:** Referem-se aos ativos corporativos que são públicos e podem ser descobertos por meio de reconhecimento do sistema de nomes de domínio e varredura de rede da Internet pública fora da rede da empresa.[3]
- **Ativos corporativos internos:** Referem-se a ativos corporativos não-públicos que só podem ser identificados por meio de varreduras de rede e reconhecimento de dentro da rede da empresa por meio de acesso autorizado autenticado ou não autenticado.[3]
- **Ativos de software:** Também chamados de software neste documento, são os programas e outras informações operacionais usados em um ativo corporativo. Os ativos de software incluem sistemas operacionais e aplicações.[3]
- **Autenticação** - processo que busca verificar a identidade digital de uma entidade de um sistema; [8]
- **Autorização** - processo que ocorre após a autenticação e que tem a função de diferenciar os privilégios atribuídos ao usuário que foi autenticado;[16]
- **Banco de dados:** Coleção organizada de dados, geralmente armazenados e acessados eletronicamente a partir de um sistema de computador. Os bancos de dados podem residir remotamente ou no local. Sistemas de gestão de banco de dados (SGBDs ou DMSs) são usados para administrar bancos de dados e não são considerados parte de um banco de dados para este documento.[3]
- **Biblioteca:** Código pré-escrito, classes, procedimentos, scripts, dados de configuração e outros, usados para desenvolver programas de software e aplicações. É projetado para auxiliar o programador e o compilador da linguagem de programação na construção e execução do software.[3]
- **Confidencialidade:** propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada a pessoa, a sistema, a órgão ou a entidades não autorizadas nem credenciadas.[2]
- **Conformidade:** Adesão a leis, regulamentos e políticas internas.[3]
- **Contas de administrador:** Contas dedicadas com privilégios escalados e usadas para gerenciar aspectos de um computador, domínio ou toda a infraestrutura de tecnologia da informação da empresa. Os subtipos comuns de contas de administrador incluem contas root, contas de administrador local e de administrador de domínio e contas de administrador de rede ou dispositivos de segurança.[3]
- **Contas de serviço:** Uma conta dedicada com privilégios escalados usada para executar aplicações e outros processos. As contas de serviço também podem ser criadas apenas

para possuir dados e arquivos de configuração. Elas não se destinam ao uso por pessoas, exceto para a execução de operações administrativas.[3]

- **Contas de usuário:** Uma identidade criada para uma pessoa em um computador ou sistema de computação. Para os fins deste documento, contas de usuário referem-se a contas de usuário “padrão” ou “interativas” com privilégios limitados e usadas para tarefas gerais, como ler e-mail e navegar na web. Contas de usuário com privilégios escalados são cobertas por contas de administrador.[3]
- **Criptografia:** Método de proteger informações convertendo-as em um código para evitar acesso não autorizado.[3]
- **Dados Corporativos:** Informações relacionadas às operações, funcionários, consumidores e parceiros de uma empresa.[3]
- **Disponibilidade:** propriedade pela qual se assegura que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados.[2]
- **Dispositivos de rede:** Dispositivos eletrônicos necessários para comunicação e interação entre dispositivos em uma rede de computadores. Os dispositivos de rede incluem pontos de acesso sem fio, firewalls, gateways físicos/virtuais, roteadores e switches. Estes dispositivos consistem em hardware físico, bem como dispositivos virtuais e baseados em nuvem. Para os fins deste documento, os dispositivos de rede são um subconjunto dos ativos corporativos.[3]
- **Dispositivos de usuário final:** Ativos de tecnologia da informação (TI) usados entre os membros de uma empresa durante o trabalho, fora do expediente ou qualquer outra finalidade. Os dispositivos de usuário final incluem dispositivos móveis e portáteis, como laptops, smartphones e tablets, bem como desktops e estações de trabalho. Para os fins deste documento, os dispositivos do usuário final são um subconjunto dos ativos corporativos.[3]
- **Dispositivos móveis de usuário final:** Pequenos dispositivos corporativos de usuário final com capacidade intrínseca sem fio, como smartphones e tablets. Dispositivos móveis de usuário final são um subconjunto de dispositivos portáteis de usuário final, incluindo laptops, que podem exigir hardware externo para conectividade. Para os fins deste documento, os dispositivos móveis de usuário final são um subconjunto dos dispositivos de usuário final.[3]
- **Dispositivos portáteis de usuário final:** Dispositivos transportáveis de usuário final que têm a capacidade de se conectar a uma rede sem fio. Para os fins deste documento, dispositivos portáteis de usuário final podem incluir laptops e dispositivos móveis, como smartphones e tablets, todos os quais são um subconjunto de ativos corporativos.[3]

- **Dispositivos remotos:** Qualquer ativo corporativo capaz de se conectar a uma rede remotamente, geralmente da Internet pública. Isso pode incluir ativos corporativos, como dispositivos de usuário final, dispositivos de rede, dispositivos não computacionais/Internet das Coisas (IoT) e servidores.[3]
- **Engenharia social:** Refere-se a uma ampla gama de atividades maliciosas realizadas por meio de interações humanas em várias plataformas, como e-mail ou telefone. Depende de manipulação psicológica para induzir os usuários a cometer erros de segurança ou fornecer informações sensíveis.[3]
- **Gestão de Provedores de Serviços:** Processo de avaliar e monitorar terceiros que fornecem serviços à empresa.[3]
- **Gerenciamento de Terceiros:** Processo de avaliar e monitorar parceiros e fornecedores que têm acesso aos sistemas da empresa.[3]
- **Governança de Privacidade:** Conjunto de práticas e diretrizes para gerenciar e proteger informações pessoais.[3]
- **Governança, Riscos e Compliance (GRC):** Estrutura para garantir que as práticas de TI de uma organização estejam alinhadas com os objetivos de negócios, enquanto gerencia riscos e cumpre regulamentações.[3]
- **Incidente de Segurança:** Qualquer evento adverso que comprometa a integridade, confidencialidade ou disponibilidade de informações.[3]
- **Infraestrutura de rede:** Refere-se a todos os recursos de uma rede que tornam possível a conectividade, a gestão, as operações comerciais e a comunicação de rede ou Internet. Consiste em hardware e software, sistemas e dispositivos e permite a computação e a comunicação entre usuários, serviços, aplicações e processos. A infraestrutura de rede pode ser em nuvem, física ou virtual.[3]
- **Integridade:** propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental. [2]
- **Interoperabilidade:** característica que se refere à capacidade de diversos sistemas e organizações trabalharem em conjunto (interoperar) de modo a garantir que pessoas, organizações e sistemas computacionais interajam para trocar informações de maneira eficaz e eficiente. [2]
- **Inventário de Ativos:** Lista detalhada de todos os ativos de TI, como hardware, software e informações.[3]
- **Malware:** software malicioso, projetado para infiltrar um sistema computacional, com a intenção de roubar dados ou danificar aplicativos ou o sistema operacional. Esse tipo de software costuma entrar em uma rede por meio de diversas atividades aprovadas pela

empresa, como e-mail ou sites. Entre os exemplos de *malware* estão os vírus, *worms*, trojans (ou cavalos de Troia), *spyware*, *adware* e *toolkits*. [8]

- **Mídia removível:** Qualquer tipo de dispositivo de armazenamento que pode ser removido de um computador enquanto o sistema está funcionando e permite que os dados sejam movidos de um sistema para outro. Exemplos de mídia removível incluem discos compactos (CDs), discos versáteis digitais (DVDs) e discos Blu-ray, backups em fita, bem como disquetes e unidades de barramento serial universal (USB). [3]
- **Phishing:** é um tipo de fraude na qual o golpista tenta obter informações pessoais e financeiras do usuário, combinando meios técnicos e engenharia social. A palavra *phishing*, do inglês “*fishing*”, é uma analogia criada pelos golpistas, em que “iscas” (mensagens eletrônicas) são usadas para “pescar” informações de usuários. [20]
- **Plano de Resposta a Incidentes:** Estratégia e procedimentos detalhados para responder a incidentes de segurança. [3]
- **Política de Privacidade:** Declaração que descreve como uma empresa coleta, usa, protege e divulga informações pessoais. [3]
- **Recuperação de Desastres:** Estratégias e procedimentos para recuperar sistemas e dados após um desastre ou falha significativa. [3]
- **Resposta a Incidentes:** Processo de identificar, responder e gerenciar um incidente de segurança. [3]
- **Retenção de Dados:** Política ou prática de manter registros de informações por um período específico. [3]
- **Segurança Cibernética:** ações voltadas para a segurança de operações, de forma a garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis. [2]
- **Segurança da Informação:** Práticas para proteger informações contra acesso, uso, divulgação, interrupção, modificação ou destruição não autorizados. [3]
- **Servidores:** Um dispositivo ou sistema que fornece recursos, dados, serviços ou programas a outros dispositivos em uma rede local ou em uma rede remota. Os servidores podem fornecer recursos e usá-los de outro sistema ao mesmo tempo. Os exemplos incluem servidores web, servidores de aplicações, servidores de e-mail e servidores de arquivos. [3]
- **Sistemas de arquivos remotos:** Permitem que uma aplicação executada em um ativo corporativo acesse arquivos armazenados em um ativo diferente. Os sistemas de arquivos remotos geralmente tornam outros recursos, como dispositivos remotos não

computacionais, acessíveis a partir de um ativo. O acesso remoto ao arquivo ocorre por meio de alguma forma de rede local, rede de longa distância, link ponto a ponto ou outro mecanismo de comunicação. Esses sistemas de arquivos são frequentemente chamados de sistemas de arquivos de rede ou sistemas de arquivos distribuídos.[3]

- **Sistemas de autenticação:** Um sistema ou mecanismo usado para identificar um usuário por meio da associação de uma solicitação de entrada a um conjunto de credenciais de identificação. As credenciais fornecidas são comparadas às de um arquivo em um banco de dados de informações do usuário autorizado em um sistema operacional local, serviço de diretório de usuário ou em um servidor de autenticação. Exemplos de sistemas de autenticação podem incluir *active directory*, autenticação multifator (MFA), biometria e tokens.[3]
- **Sistemas de autorização:** Um sistema ou mecanismo usado para determinar os níveis de acesso ou privilégios de usuário/consumidor relacionados aos recursos do sistema, incluindo arquivos, serviços, programas de computador, dados e recursos de aplicações. Um sistema de autorização concede ou nega acesso a um recurso com base na identidade do usuário. Exemplos de sistemas de autorização podem incluir *active directory*, listas de controle de acesso e listas de controle de acesso baseadas em funções.[3]
- **Telecomunicações:** Transmissão e recepção de informações por meios eletrônicos.
- **Terceiros:** Fornecedores, parceiros ou qualquer outra organização ou indivíduo que não faz parte da empresa principal.[3]
- **Vulnerabilidade:** conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou por uma organização, os quais podem ser evitados por uma ação interna de segurança da informação.[2]

Anexo 1 - Resumo dos Objetivos do Guia

# Objetivo	Capítulo	Nome do Objetivo	Controle
01	Inventário de Ativos	Estabelecer uma Política de Gestão Ativos	S/N
02	Proteção de Dados	Estabelecer uma Política de Proteção de Dados	S/N
03	Configuração Segura de Ativos e Gestão de Vulnerabilidades	Estabelecer uma Política de configuração segura de ativos	S/N
04		Estabelecer uma Política de Gestão de Vulnerabilidade e Remediação	S/N
05	Controle de Acesso e Contas	Estabelecer uma Política de Controle de Acesso e Contas.	S/N
06	Monitoramento de atividades e Gestão de Registros de Auditoria	Estabelecer uma Política de Monitoramento de Atividades na Rede	S/N
07		Estabelecer uma Política de Gestão de Registros(log) de Auditoria	S/N
08	Backup e Recuperação de Dados	Estabelecer uma Política de Backup e Recuperação de Dados	S/N
09	Conscientização dos Funcionários sobre Segurança Cibernética	Estabelecer um Programa de Conscientização para os Funcionários sobre Segurança Cibernética	S/N
010	Conscientização dos Consumidores sobre Segurança Cibernética	Estabelecer um Programa de Conscientização para os Consumidores sobre Segurança Cibernética	S/N
011	Segurança Física	Estabelecer uma Política de Segurança Física para Sistemas e Dados.	S/N
012	Plano de Resposta a Incidentes	Estabelecer um Plano de Resposta a Incidentes	S/N
013	Política de Segurança da Cibernética	Estabelecer uma Política de Segurança Cibernética	S/N

Anexo 2 - Resumo das Medidas do Guia

# Medida	Capítulo	Número do Medida	Nome da Medida	Verificação
M1	Inventário de Ativos	1.1	Estabelecer e manter um inventário detalhado de ativos corporativos	S/N
M2		1.2	Tratar ativos não autorizados	S/N
M3		1.3	Estabelecer e manter um inventário de software	S/N
M4		1.4	Assegurar que o software autorizado seja atualmente suportado	S/N
M5		1.5	Tratar o software não autorizado	S/N
M6		1.6	Estabelecer e manter um inventário de contas	S/N
M7		1.7	Estabelecer e manter um inventário de provedores de serviços	S/N
M8	Proteção de Dados	2.1	Estabelecer e manter um processo de gestão de dados	S/N
M9		2.2	Estabelecer e manter um inventário de dados	S/N
M10		2.3	Configurar listas de controle de acesso a dados	S/N
M11		2.4	Aplicar retenção de dados	S/N
M12		2.5	Descartar dados com segurança	S/N
M13		2.6	Criptografar dados sensíveis em dispositivos de usuário final	S/N
M14	Configuração Segura de Ativos e Gestão de Vulnerabilidades	3.1	Estabelecer e manter um processo de configuração segura	S/N
M15		3.2	Estabelecer e manter um processo de configuração segura para a infraestrutura de rede	S/N

M16		3.3	Configurar o bloqueio automático de sessão nos ativos corporativos	S/N
M17		3.4	Implementar e gerenciar um firewall nos servidores	S/N
M18		3.5	Implementar e gerenciar um firewall nos dispositivos de usuário final	S/N
M19		3.6	Gerenciar com segurança os ativos e softwares corporativos	S/N
M20		3.7	Gerenciar contas padrão nos ativos e softwares corporativos	S/N
M21		3.8	Garantir o uso apenas de navegadores e consumidores de e-mail suportados plenamente	S/N
M22		3.9	Usar serviços de filtragem de DNS	S/N
M23		3.10	Instalar e manter um software anti- <i>malware</i>	S/N
M24		3.11	Configurar atualizações automáticas de assinatura anti- <i>malware</i>	S/N
M25		3.12	Desabilitar a execução e reprodução automática para mídias removíveis	S/N
M26		3.13	Acelerar a transição completa para o IPv6 o mais breve possível	S/N
M27		3.14	Estabelecer e manter um processo de gestão de vulnerabilidade	S/N
M28		3.15	Estabelecer e manter um processo de remediação	S/N
M29		3.16	Manter sistemas e aplicações atualizados (gestão automatizada de patches)	S/N
M30	Controle de Acesso e Contas	4.1	Utilizar senhas fortes e exclusivas	S/N
M31		4.2	Exigir mudanças periódicas de senhas	S/N
M32		4.3	Não compartilhar senhas	S/N
M33		4.4	Não armazenar senhas em locais de fácil acesso	S/N

M34		4.5	Desabilitar contas inativas	S/N
M35		4.6	Limitar as permissões de administrador exclusivamente a contas designadas com esse propósito	S/N
M36		4.7	Estabelecer um processo de concessão e revogação de acesso	S/N
M37		4.8	Exigir MFA onde for necessário	S/N
M38	Monitoramento de atividades e Gestão de Vulnerabilidades e Registros	5.1	Implementar monitoramento de atividades	S/N
M39		5.2	Estabelecer e manter um processo de gestão de registros(log) de auditoria	S/N
M40		5.3	Coletar registros(log) de auditoria	S/N
M41		5.4	Garantir o armazenamento adequado dos registros(log) de auditoria	S/N
M42		5.5	Assegurar que a infraestrutura de rede esteja atualizada	S/N
M43		5.6	Monitorar atividades de terceiros	S/N
M44	Backup e Recuperação de Dados	6.1	Estabelecer e manter um processo de recuperação de dados	S/N
M45		6.2	Fazer backup regularmente e automatizado	S/N
M46		6.3	Proteger os dados de recuperação	S/N
M47		6.4	Estabelecer e manter uma instância isolada de dados de recuperação	S/N
M48		6.5	Verificar se os Backups estão Funcionando Corretamente	S/N
M49	Conscientização dos Funcionários sobre Segurança Cibernética	7.1	Estabelecer e manter um programa de conscientização dos funcionários de segurança cibernética	S/N
M50		7.2	Conhecer as principais ameaças cibernéticas	S/N
M51		7.3	Conscientizar sobre as melhores práticas de autenticação	S/N

M52		7.4	Treinar membros da força de trabalho sobre as causas da exposição não intencional de dados	S/N
M53		7.5	Conscientizar sobre o plano de resposta a incidentes	S/N
M54		7.6	Treinar a força de trabalho sobre como identificar e comunicar se os seus ativos corporativos não estão atualizados corretamente	S/N
M55		7.7	Treinar a força de trabalho sobre os perigos de se conectar e transmitir dados corporativos em redes inseguras	S/N
M56		7.8	Conscientizar sobre as fragilidades críticas em equipamentos instalados	S/N
M57		7.9	Fornecer treinamento em segurança cibernética para terceiros	S/N
M58	Conscientização dos Consumidores sobre Segurança Cibernética	8.1	Estabelecer e manter um programa de conscientização de segurança	S/N
M59		8.2	Explorar diferentes materiais e abordagens, reconhecendo as diferenças e as necessidades de diversos grupos sociais	S/N
M60		8.3	Conhecer as principais ameaças cibernéticas (ex: engenharia social)	S/N
M61		8.4	Conscientizar sobre as melhores práticas de autenticação	S/N
M62		8.5	Educar os consumidores sobre os riscos de se conectar e transmitir dados em redes inseguras	S/N
M63	Segurança Física	9.1	Estabelecer controle de acesso físico	S/N
M64		9.2	Estabelecer monitoramento por câmeras	S/N
M65		9.3	Estabelecer proteção de equipamentos	S/N
M66		9.4	Estabelecer política de mesa limpa e tela limpa	S/N
M67	Plano de Resposta	10.1	Designar pessoal para gerenciar tratamento de incidentes	S/N

M68		10.2	Estabelecer e manter informações de contato para relatar incidentes de segurança	S/N
M69		10.3	Estabelecer e manter um processo corporativo para relatar incidentes	S/N
M70	Política de Segurança Cibernética	11.1	Definir segurança cibernética	S/N
M71		11.2	Estabelecer objetivos e princípios de segurança cibernética	S/N
M72		11.3	Estabelecer diretrizes e requisitos de segurança cibernética	S/N
M73		11.4	Atribuir responsabilidades de segurança da cibernética	S/N
M74		11.5	Definir as sanções disciplinares	S/N

