CIS Center for Internet Security®

CIS Controls

Controles CIS

Versão 8

V8

Controles CIS Versão 8

Maio 2021

Agradecimentos

O CIS gostaria de agradecer aos muitos especialistas em segurança que doaram seu tempo e talento para suportar os Controles CIS e outros trabalhos do CIS. Os produtos CIS representam o esforço de um verdadeiro exército de voluntários de toda a indústria, generosamente doando seu tempo e talento em nome de uma experiência online mais segura para todos.

Reconhecimento

O CIS gostaria de expressar nosso agradecimento a Modulo Security por seu trabalho nesta iniciativa dos Controles CIS Versão 8. A Modulo Security gentilmente cedeu o tempo e profissionalismo de seus colaboradores para se tornar promotora e apoiadora nacional da metodologia dos Controles CIS. Seu trabalho de tradução dos Controles CIS Versão 8 torna-os mais facilmente disponíveis para serem adotados e implementados por empresas brasileiras para reforçar sua defesa cibernética. Este guia padroniza ordens, prioridades e medidas dos esforços das empresas brasileiras de segurança cibernética. Graças a Modulo Security, a outros voluntários profissionais de TI globais e à equipe dos Controles CIS, continuaremos a trabalhar juntos para construir um ciberespaço seguro e resiliente.

Conteúdo

Glossário

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.
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.
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.
Sistemas de autorização	Um sistema ou mecanismo usado para determinar os níveis de acesso ou privilégios de usuário/cliente 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.
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).
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.
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.
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.

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.
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.
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.
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.
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.
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.
Dispositivos não computacionais/Internet das Coisas (IoT)	Dispositivos incorporados com sensores, software e outras tecnologias com a finalidade de conectar, armazenar e trocar dados com outros dispositivos e sistemas pela Internet. Embora esses dispositivos não sejam usados para processos computacionais, eles oferecem suporte à capacidade de uma empresa de conduzir processos de negócios. Exemplos destes dispositivos incluem impressoras, telas inteligentes, sensores de segurança física, sistemas de controle industrial e sensores de tecnologia da informação. Para os fins deste documento, os dispositivos não computacionais/IoT são um subconjunto dos ativos corporativos.
Sistema operacional	Software dos ativos corporativos que gerencia recursos de hardware e software do computador e fornece serviços comuns para programas. Os sistemas operacionais são considerados ativos de software e podem ser simples ou multitarefa, de um ou vários usuários, distribuídos, modelados, embarcados, em tempo real e bibliotecas.
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.
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.

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.
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.
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).
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 email e servidores de arquivos.
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.
Serviços	Refere-se a uma funcionalidade de software ou um conjunto de funcionalidades de software, como a recuperação de informações especificadas ou a execução de um conjunto de operações. Os serviços fornecem um mecanismo para permitir o acesso a um ou mais recursos, onde o acesso é fornecido usando uma interface determinada e com base na identidade do solicitante de acordo com as políticas de uso da empresa.
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.
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.
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.
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.

Acrônimos e abreviações (em inglês)

AAA	Authentication, Authorization, and Auditing
ACL	Access Control List
AD	Active Directory
AoC	Attestation of Compliance
API	Application Programming Interface
BEC	Business Email Compromise
C2	Command and Control
CCE	Common Configuration Enumeration
CDM	Community Defense Model
CIA	Confidentiality, Integrity, and Availability
CIS	Center for Internet Security
CIS –CAT	CIS Configuration Assessment Tool
COTS	Commercial off-the-Shelf
CPE	Common Platform Enumeration
CREST	Council of Registered Security Testers
CSA	Cloud Security Alliance
CSP	Cloud Service Provider
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DBIR	Data Breach Investigations Report
DEP	Data Execution Prevention
DG	Development Group
DHCP	Dynamic Host Configuration Protocol
DKIM	DomainKeys Identified Mail
DLP	Data Loss Prevention
DMARC	Domain-based Message Authentication, Reporting, and Conformance
DMS	Database Management System
DNS	Domain Name System
DPI	Deep Packet Inspection
EDR	Endpoint Detection and Response
EOL	End of Life
FFIEC	Federal Financial Institutions Examination Council
FISMA	Federal Information Security Modernization Act
GRC	Governance Risk and Compliance
HECVAT	Higher Education Community Vendor Assessment Toolkit
HIPAA	Health Insurance Portability and Accountability Act
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
IDS	Intrusion Detection System
IG	Implementation Group
IOCs	Indicators of Compromise
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
ISAC	Information Sharing and Analysis Center
ISO	International Organization for Standardization
IT	Information Technology
LotL	Living off the Land
MDM	Mobile Device Management
MFA	Multi-Factor Authentication
MITRE ATT&CK	MITRE Adversarial Tactics, Techniques, and Common Knowledge®
MS-ISAC	Multi-State Information Sharing and Analysis Center
NaaS	Network-as-a-Service
NCSA	National Cyber Security Alliance
NIDS	Network Intrusion Detection System
NIST	National Institute of Standards and Technology
OS	Operating System
OSS	Open Source Software
OVAL	Open Vulnerability and Assessment Language
OWASP	Open Web Application Security Project
PaaS	Platform as a Service
PAM	Privileged Access Management
PCI	Payment Card Industry

SaaS	Software as a Service
SAFECode	Software Assurance Forum for Excellence in Code
SCADA	Supervisory Control and Data Acquisition
SCAP	Security Content Automation Protocol
SIEM	Security Information and Event Management
SIP	System Integrity Protection
SMS	Short Messaging Service
SOC	Security Operations Center
SOC 2	Service Organization Control 2
SPAM	Something Posing as Mail
SPF	Sender Policy Framework
SQL	Structured Query Language
SSDF	Secure Software Development Framework
SSH	Secure Shell
SSO	Single Sign-On
Telnet	Teletype Network
TLS	Transport Layer Security
TTPs	Tactics, Techniques, and Procedures
U.K.	United Kingdom
URL	Uniform Resource Locator
USB	Universal Serial Bus
VPN	Virtual Private Network
WDEG	Windows Defender Exploit Guard
WPA2	Wi-Fi Protected Access 2
XCCDF	Extensible Configuration Checklist Description Format

Introdução

Os Controles CIS® começaram como uma atividade básica simples para identificar os ataques cibernéticos mais comum e importantes do mundo real que afetam as empresas todos os dias, traduzir esse conhecimento e experiência em ações positivas e construtivas para os defensores e, em seguida, compartilhar essas informações com um público mais amplo. Os objetivos originais eram modestos—ajudar as pessoas e empresas a concentrarem sua atenção e darem início aos passos mais importantes para se defenderem dos ataques que realmente importam.

Liderados pelo Center for Internet Security® (CIS®), os Controles CIS amadureceram e se tornaram uma comunidade internacional de indivíduos e instituições voluntários que:

- Compartilham percepções sobre ataques e invasores, identificam as causas básicas e as traduzem em classes de ação defensiva
- Criam e compartilham ferramentas, ajudas de trabalho e histórias de adoção e solução de problemas
- Mapeiam os controles CIS com estruturas regulatórias e de compliance, a fim de garantir o alinhamento e trazer prioridade e foco para eles
- Identificam problemas e barreiras comuns (como avaliação inicial e roteiros de implementação), e as resolvem como uma comunidade

Os Controles CIS refletem o conhecimento combinado de especialistas de todas as partes do ecossistema (empresas, governos, indivíduos), com todas as funções (times de respostas e analistas de ameaças, tecnólogos, operadores e defensores de tecnologia da informação (TI), pesquisadores de vulnerabilidades, fabricantes de ferramentas, provedores de soluções, usuários, formuladores de políticas, auditores, etc.) e em muitos setores (governo, poder, defesa, finanças, transporte, academia, consultoria, segurança, TI, etc.), que se uniram para criar, adotar e apoiar os Controles CIS.

Evolução dos Controles CIS

Os Controles CIS começaram como muitas atividades semelhantes—reunimos especialistas, compartilhamos e discutimos até chegarmos a um acordo. Isso pode ser muito valioso, dependendo das pessoas envolvidas e de suas experiências. Ao documentar e compartilhar os resultados, todas as empresas podem então se beneficiar do trabalho de pessoas que não podem contratar ou mesmo conhecer. Você pode melhorar os resultados (e sua confiança neles) selecionando especialistas que representam uma ampla gama de conhecimentos, trazendo consistência ao processo e garantindo o uso das melhores informações disponíveis (especialmente sobre ataques). No final das contas, você ainda depende do bom julgamento de um grupo relativamente pequeno de pessoas, consolidados de forma informal e relatos.

No CIS, temos percorrido um caminho de vários anos para trazer mais dados, rigor e transparência ao processo de recomendações de melhores práticas (Benchmarks CIS™ e Controles CIS). Todos esses elementos são essenciais para o amadurecimento de uma ciência para fundamentar a defesa cibernética; e, necessários para permitir a adaptação e "negociação" de ações de segurança aplicáveis em casos específicos, e conforme exigido pelos frameworks específicos de segurança, regulamentações e esquemas de supervisão semelhantes.

Nas primeiras versões dos Controles CIS, usamos uma lista padrão de ataques conhecidos publicamente como um teste simples e informal da utilidade de recomendações específicas. A partir de 2013, trabalhamos com a equipe do Verizon Data Breach Investigations Report (DBIR) para mapear os resultados de sua análise de dados em grande escala diretamente para os Controles CIS, como uma forma de combinar seus resumos de ataques em um programa padrão para melhoria defensiva.

O CIS lançou recentemente o Community Defense Model (CDM), que é nossa abordagem mais baseada em dados até agora. Em sua versão inicial, o CDM analisa as conclusões do DBIR da Verizon mais recentes, juntamente com os dados do Multi-State Information Sharing and Analysis Center®(MS-ISAC®), para identificar o que acreditamos ser os cinco mais importantes tipos de ataques. Descrevemos esses ataques usando o framework MITRE Adversarial Tactics, Techniques e Common Knowledge® (MITRE ATT&CK®) para criar padrões de ataque (ou combinações específicas de táticas e técnicas usadas nesses ataques). Isso nos permite analisar o valor das ações defensivas individuais (ou seja, Medidas de Segurança[1]) contra esses ataques. Especificamente, também fornece uma maneira consistente e explicável de examinar o valor de segurança de um determinado conjunto de ações defensivas em todo o ciclo de vida do invasor e fornece uma base para estratégias tais como defesa em profundidade. Os detalhes desta análise estão disponíveis no website do CIS. O resultado final é que demos um passo importante no sentido de identificar o valor de segurança dos Controles CIS, ou qualquer subconjunto deles. Embora essas ideias ainda estejam evoluindo, no CIS estamos comprometidos com a ideia de recomendações de segurança baseadas em dados, apresentadas de forma transparente. Para obter informações adicionais, consulte https://www.cisecurity.org/controls/v8/.

Essas atividades garantem que as Melhores Práticas de Segurança do CIS (que incluem os Controles CIS e Benchmarks CIS) sejam mais do que uma lista de verificação de "coisas boas a fazer" ou "coisas que podem ajudar"; em vez disso, são um conjunto de ações prescritivas, priorizadas e altamente focadas que possuem uma rede de suporte da comunidade para torná-las implementáveis, utilizáveis, escaláveis e alinhadas com todos os requisitos de segurança da indústria ou do governo.

[1] "Medidas de Segurança" eram conhecidas como "Sub-Controles" antes da versão 8 dos Controles CIS.

Esta versão dos Controles CIS

Quando começamos o trabalho de uma nova versão, primeiro estabelecemos os "princípios de design" que serão usados para orientar o processo. Eles servem como uma "pedra de toque" de decisão para nos lembrar do que é realmente importante e dos objetivos dos Controles CIS. Embora tenham sido bastante consistentes desde as primeiras versões dos Controles CIS, refinamos nosso pensamento nas últimas duas versões para nos concentrar no papel que os Controles CIS desempenham no quadro geral da segurança corporativa.

Nossos princípios de design incluem:

- Ataque Informa a Defesa
  - Os Controles CIS foram selecionados, descartados e priorizados com base nos dados e no conhecimento específico do comportamento do invasor e como evitá-lo.
- Foco
  - Ajudar os defensores a identificar as coisas mais críticas que precisam fazer para impedir os ataques mais importantes
  - Evitar a tentação de resolver todos os problemas de segurança—evitar adicionar "coisas boas a fazer" ou "coisas que você *poderia* fazer"
- Viável
  - Todas as recomendações individuais (Medidas de Segurança) devem ser específicas e práticas para implementar
- Mensurável
  - Todos os controles CIS, especialmente para o Grupo de Implementação 1, devem ser mensuráveis
  - Simplificar ou remover linguagem ambígua para evitar interpretação inconsistente.
  - Algumas Medidas de Segurança podem ter um limite
- Alinhamento
  - Criar e demonstrar "coexistência pacífica" com outras estruturas de governança, regulamentações, esquemas de gestão de processos, frameworks e estruturas
  - Cooperar e apontar para padrões independentes existentes e recomendações de segurança onde existirem, por exemplo, National Institute of Standards and Technology® (NIST®), Cloud Security Alliance (CSA), Software Assurance Forum for Excellence in Code (SAFECode), ATT&CK, Open Web Application Security Project® (OWASP®)

Além disso, desde a versão 7, todos nós vimos mudanças significativas na tecnologia e no ecossistema de segurança cibernética. O movimento para a computação baseada em nuvem, virtualização, mobilidade, terceirização, trabalho em casa e mudanças nas táticas do invasor têm sido centrais em todas as discussões. Dispositivos físicos, fronteiras fixas e ilhas discretas de implementação de segurança são menos importantes e, portanto, refletimos isso na Versão 8, por meio de terminologia revisada e agrupamentos das Medidas de Segurança. Além disso, para orientar os usuários na implementação da Versão 8, o CIS criou um glossário para remover a ambiguidade da terminologia. Algumas ideias foram combinadas ou agrupadas de maneira diferente para refletir mais naturalmente a evolução da tecnologia, em vez de como as equipes ou responsabilidades corporativas podem ser organizadas, e sempre se referindo aos nossos princípios orientadores.

O texto do documento Controles CIS é apenas um passo de um processo para projetar, implementar, medir, relatar e gerenciar a segurança corporativa. Levando todo esse fluxo de trabalho em consideração enquanto escrevíamos os Controles CIS, conseguimos oferecer suporte a todo o processo de gestão empresarial por meio de: nos certificando que cada Medida de Segurança solicite "uma coisa", sempre que possível, de uma forma que seja clara e exija o mínimo de interpretação; concentrando em ações mensuráveis e definição da medição como parte do processo; e, simplificando a linguagem para evitar duplicações.

No CIS, sempre tentamos estar muito conscientes do equilíbrio entre abordar os tópicos atuais e a estabilidade de um programa geral de melhoria defensiva. Sempre tentamos nos concentrar nos fundamentos de uma boa defesa cibernética—e sempre tentamos manter nossos olhos nas novas tecnologias defensivas emergentes—enquanto evitamos os "brinquedos novos e brilhantes" ou tecnologia complexa que está fora do alcance da maioria das empresas.

O Ecossistema de Controles CIS ("Não se trata da lista")

Quer você use os Controles CIS e/ou outra forma de orientar seu programa de melhoria de segurança, você deve reconhecer que "não se trata da lista". Você pode obter uma lista confiável de recomendações de segurança de várias fontes—é melhor pensar na lista como um ponto de partida. É importante procurar o ecossistema que cresce em torno da lista. Onde possa obter treinamentos, informações complementares, explicações; como outros implementaram e usaram essas recomendações; há um mercado de ferramentas e serviços de fornecedores para escolher; como medir o progresso ou maturidade; como isso se alinha com a miríade de estruturas regulatórias e de conformidade que se aplicam a mim? O verdadeiro poder dos Controles CIS não é criar a melhor lista, mas sim aproveitar a experiência de uma comunidade de indivíduos e empresas para realmente fazer melhorias na segurança por meio do compartilhamento de ideias, ferramentas, lições e ações coletivas.

Para apoiar isso, o CIS atua como um catalisador e uma câmara de compensação para nos ajudar a aprender uns com os outros. Desde a versão 6, tem havido uma explosão de informações, produtos e serviços complementares disponíveis no CIS e na indústria em geral. Entre em contato com o CIS para os seguintes tipos de ajuda de trabalho e outros materiais de suporte, https://www.cisecurity.org/controls/v8/:

- Mapeamentos dos controles CIS para uma grande variedade de Frameworks de Gestão de Riscos (como NIST®, Federal Information Security Modernization Act (FISMA), International Organization for Standardization (ISO), etc.)

- Casos de uso de adoção nas empresas
- Uma lista de referências contínuas aos Controles CIS em padrões nacionais e internacionais, legislação e regulamentação estadual e nacional, associações comerciais e de profissionais, etc.
- Informações sob medida para pequenas e médias empresas
- Medidas e métricas para os Controles CIS
- Indicadores para white papers de fornecedores e outros materiais que apoiam os Controles CIS
- Documentação sobre o alinhamento com o NIST®. Cybersecurity Framework

Como Começar

Historicamente, os Controles CIS foram ordenados em sequência para focalizar as atividades de segurança cibernética de uma empresa, com um subconjunto dos primeiros seis Controles CIS referidos como "higiene cibernética. " No entanto, isso provou ser muito simplista. As empresas, especialmente as pequenas, podem ter dificuldades com algumas das primeiras Medidas de Segurança e nunca conseguir implementar os controles CIS posteriores (por exemplo, ter uma estratégia de backup para ajudar na recuperação de ransomware). Como resultado, a partir da versão 7.1, criamos Grupos de Implementação de Controles CIS (IGs) como nossa nova orientação recomendada para priorizar a implementação.

Os IGs dos Controles CIS são categorias autoavaliadas para empresas. Cada IG identifica um subconjunto dos Controles CIS que a comunidade avaliou amplamente para serem aplicáveis a uma empresa com um perfil de risco e recursos semelhantes para implementação. Esses IGs representam uma visão horizontal dos Controles CIS adaptados a diferentes tipos de empresas. Especificamente, definimos IG1 como "higiene cibernética básica", o conjunto básico de Medidas de Segurança de defesa cibernética que toda empresa deve aplicar para se proteger contra os ataques mais comuns [https://www.cisecurity.org/controls/v8/]. Cada IG então se baseia no anterior: IG2 inclui IG1, e IG3 inclui todas as Medidas de Segurança CIS em IG1 e IG2.

Uso ou Transição de Versões Anteriores dos Controles CIS

Acreditamos que esta versão 8 dos Controles CIS seja a melhor que já produzimos. Também apreciamos que as empresas que estão usando ativamente versões anteriores dos Controles CIS como uma parte fundamental de sua estratégia defensiva podem relutar em mudar para a versão 8. Nossa recomendação é que se você estiver usando a versão 7 ou a versão 7.1, você está seguindo um plano de segurança eficaz e utilizável e, com o tempo, você deve considerar a mudança para a versão 8. Se estiver usando a versão 6 (ou anterior), nossa recomendação é que você deve começar a planejar uma transição para a versão 8 assim que possível.

Para versões anteriores dos Controles CIS, fomos capazes de fornecer apenas as ferramentas mais simples para ajudar na transição destas versões anteriores, basicamente um registro de alterações baseado em planilha. Para a versão 8, adotamos uma abordagem muito mais holística e trabalhamos com vários parceiros para garantir que o ecossistema de Controles CIS esteja pronto para oferecer suporte à sua transição, https://www.cisecurity.org/controls/v8/.

Estrutura dos Controles CIS

A apresentação de cada controle neste documento inclui os seguintes elementos:

- **Visão geral:** Uma breve descrição da intenção do Controle e sua utilidade como ação defensiva.
- **Por que este controle é crítico?** Uma descrição da importância deste Controle no bloqueio, mitigação ou identificação de ataques, e uma explicação de como os invasores exploram ativamente a ausência deste Controle
- **Procedimentos e ferramentas:** Uma descrição mais técnica dos processos e tecnologias que permitem a implementação e automação deste Controle
- **Medidas de Segurança:** uma tabela das ações específicas que as empresas devem realizar para implementar o Controle

Perfis

IG1

Uma empresa IG1 é de pequeno a médio porte, com experiência limitada em TI e segurança cibernética dedicada à proteção de ativos e pessoal de TI. A principal preocupação dessas empresas é manter o negócio operacional, pois têm uma tolerância limitada para o tempo de paralisação. A sensibilidade dos dados que estão tentando proteger é baixa e envolve principalmente informações financeiras e de funcionários.

As Medidas de Segurança selecionadas para IG1 devem ser implementáveis com experiência limitada em segurança cibernética e destinadas a impedir ataques gerais não direcionados. Essas proteções também são tipicamente projetadas para funcionar em conjunto com soluções pequenas e domésticas de hardware e software (comercial off-the-shelf—COTS).

IG2 (Inclui IG1)

Uma empresa IG2 emprega indivíduos responsáveis por gerenciar e proteger a infraestrutura de TI. Essas empresas oferecem suporte a vários departamentos com diferentes perfis de risco com base na função e na missão do trabalho. Pequenas unidades da empresa podem ter encargos de conformidade regulatória. As empresas IG2 geralmente armazenam e processam informações confidenciais de clientes ou empresas e podem resistir a curtas interrupções de serviço. Uma grande preocupação é a perda de confiança do público se ocorrer uma violação.

As Medidas de Segurança selecionadas para IG2 ajudam as equipes de segurança a lidar com o aumento da complexidade operacional. Algumas proteções dependerão de tecnologia de nível empresarial e conhecimento especializado para instalar e configurar adequadamente.

IG3 (Inclui IG1 e IG2)

Uma empresa IG3 emprega especialistas em segurança especializados nas diferentes facetas da segurança cibernética (por exemplo, gestão de riscos, teste de invasão, segurança de aplicações). Os ativos e dados do IG3 contêm informações ou funções confidenciais que estão sujeitas à supervisão regulatória e de conformidade. Uma empresa IG3 deve abordar a disponibilidade dos serviços e a confidencialidade e integridade dos dados sensíveis. Ataques bem-sucedidos podem causar danos significativos ao bem público.

As Medidas de Segurança selecionadas para IG3 devem diminuir os ataques direcionados de um adversário sofisticado e reduzir o impacto dos ataques zero-day.

CONTROLE 01

Inventário e controle de ativos corporativos

SAFEGUARDS TOTAL	5	IG1	2/5	IG2	4/5	IG3	5/5

Visão geral

Gestão ativa (inventariar, rastrear e corrigir) de todos os ativos corporativos (dispositivos de usuário final, incluindo portáteis e móveis; dispositivos de rede; dispositivos não computacionais; Internet das Coisas (IoT); e servidores) conectados fisicamente à infraestrutura, virtualmente, remotamente, e aqueles em ambientes de nuvem, para saber com precisão a totalidade dos ativos que precisam ser monitorados e protegidos dentro da empresa. Isso também ajudará na identificação de ativos não autorizados e não gerenciados para removê-los ou remediá-los.

Por que este controle é crítico?

As empresas não podem defender o que não sabem que possuem. A gestão do controle de todos os ativos corporativos também desempenha um papel crítico no monitoramento de segurança, resposta a incidentes, backup e recuperação de sistemas. As empresas devem saber quais dados são essenciais para elas, e a gestão adequada de ativos ajudará a identificar os ativos corporativos que mantêm ou gerenciam esses dados críticos, para que os controles de segurança apropriados possam ser aplicados.

Atacantes externos estão varrendo continuamente o espaço de endereçamento da Internet de empresas alvo, seja base local ou na nuvem, identificando ativos possivelmente desprotegidos conectados à rede corporativa. Os atacantes podem tirar proveito de novos ativos instalados, mas ainda não configurados e corrigidos com segurança. Internamente, ativos não identificados também podem ter configurações de segurança fracas que podem torná-los vulneráveis a malware baseado na web ou e-mail e os adversários podem aproveitar as configurações de segurança fracas para atravessar a rede, uma vez que estão dentro.

Ativos adicionais que se conectam à rede corporativa (por exemplo, sistemas de demonstração, sistemas de teste temporários, redes de convidados) devem ser identificados e / ou isolados para evitar que o acesso de adversários afete a segurança das operações da empresa.

Empresas grandes, complexas e dinâmicas, compreensivelmente, lutam com o desafio de gerenciar ambientes complexos e em rápida mudança. No entanto, os atacantes têm mostrado capacidade, paciência e disposição para "inventariar e controlar" nossos ativos corporativos em uma enorme escala de forma a apoiar suas oportunidades.

Outro desafio é que os dispositivos portáteis do usuário final se conectam periodicamente a uma rede e depois desaparecem, tornando o inventário dos ativos disponíveis atualmente muito dinâmico. Da mesma forma, ambientes em nuvem e máquinas virtuais podem ser difíceis de rastrear em inventários de ativos quando eles são desligados ou pausados.

Outro benefício da gestão completa de ativos corporativos é o suporte à resposta a incidentes, tanto ao investigar a origem do tráfego de rede de um ativo na rede quanto ao identificar todos os ativos potencialmente vulneráveis ou impactados, de tipo ou localização semelhante, durante um incidente.

Procedimentos e ferramentas

Este Controle CIS requer ações técnicas e processuais, conjugadas em um processo que presta contas e gerencia o inventário de ativos corporativos e todos os dados associados ao longo de seu ciclo de vida. Também se vincula à governança de negócios por meio do estabelecimento de proprietários de dados/ativos que são responsáveis por cada componente de um processo de negócios. As empresas podem usar produtos corporativos abrangentes e em grande escala para manter inventários de ativos de TI. As empresas menores podem aproveitar as ferramentas de segurança já instaladas nos ativos corporativos, ou usadas na rede, para coletar esses dados. Isso inclui fazer uma varredura de descoberta da rede com um scanner de vulnerabilidades; revisar logs de anti-malware, logs de portais de segurança de endpoint, logs de rede de switches ou logs de autenticação; e gerenciar os resultados em uma planilha ou banco de dados.

Manter uma visão atual e precisa dos ativos corporativos é um processo contínuo e dinâmico. Mesmo para empresas, raramente há uma única fonte confiável, pois os ativos corporativos nem sempre são fornecidos ou instalados pelo departamento de TI. A realidade é que uma variedade de fontes precisa ser "coletada" para determinar uma conta de alta confiabilidade dos ativos corporativos. As empresas podem realizar varreduras ativamente em uma base regular, enviando uma variedade de diferentes tipos de pacotes para identificar ativos conectados à rede. Além das fontes de ativos mencionadas acima para pequenas empresas, empresas maiores podem coletar dados de portais de nuvem e registros de plataformas corporativas, como: Active Directory (AD), Single Sign-On (SSO), Multi-Factor Authentication (MFA), Virtual Private Network (VPN), Intrusion Detection System (IDS) ou Deep Packet Inspection (DPI), Mobile Device Management (MDM) e ferramentas de varredura de vulnerabilidades. Bancos de dados proprietários de inventário, rastreamento de pedido de compra e listas de inventário locais são outras fontes de dados para determinar quais dispositivos estão conectados. Existem ferramentas e métodos que normalizam esses dados para identificar dispositivos únicos entre essas fontes.

→ **Para obter orientações específicas sobre nuvem, consulte o CIS Controls Cloud Companion Guia:** https://www.cisecurity.org/controls/v8/

→ **Para obter orientação sobre tablet e smartphone, consulte o CIS Controls Mobile Companion Guia:** https://www.cisecurity.org/controls/v8/

→ **Para obter orientação sobre IoT, consulte o CIS Controls Internet of Things Companion Guia:** https://www.cisecurity.org/controls/v8/

→ **Para orientação de Sistemas de Controle Industrial (ICS), consulte o CIS Controls ICS Guia de implementação:** https://www.cisecurity.org/controls/v8/

Medidas de Segurança

MEDIDAS DE SEGURANÇA	TÍTULO DA MEDIDA DE SEGURANÇA/ DESCRIÇÃO DA MEDIDA DE SEGURANÇA	TIPO DE ATIVO	FUNÇÃO DE SEGURANÇA	IG1	IG2	IG3
1.1	**Estabelecer e manter um inventário detalhado de ativos corporativos** Estabeleça e mantenha um inventário preciso, detalhado e atualizado de todos os ativos corporativos com potencial para armazenar ou processar dados, incluindo: dispositivos de usuário final (incluindo portáteis e móveis), dispositivos de rede, dispositivos não computacionais/IoT e servidores. Certifique-se de que o inventário registre o endereço de rede (se estático), endereço de hardware, nome da máquina, proprietário do ativo de dados, departamento para cada ativo e se o ativo foi aprovado para se conectar à rede. Para dispositivos móveis de usuário final, as ferramentas do tipo MDM podem oferecer suporte a esse processo, quando apropriado. Este inventário inclui ativos conectados à infraestrutura fisicamente, virtualmente, remotamente e aqueles dentro dos ambientes de nuvem. Além disso, inclui ativos que são regularmente conectados à infraestrutura de rede corporativa, mesmo que não estejam sob o controle da empresa. Revise e atualize o inventário de todos os ativos corporativos semestralmente ou com mais frequência.	Dispositivo	Identificar	●	●	●
1.2	**Endereçar ativos não autorizados** Assegure que exista um processo para lidar com ativos não autorizados semanalmente. A empresa pode escolher remover o ativo da rede, negar que o ativo se conecte remotamente à rede ou colocar o ativo em quarentena.	Dispositivo	Responder	●	●	●
1.3	**Usar uma ferramenta de descoberta ativa** Utilize uma ferramenta de descoberta ativa para identificar ativos conectados à rede corporativa. Configure a ferramenta de descoberta ativa para executar diariamente ou com mais frequência.	Dispositivo	Detectar		●	●
1.4	**Usar o Dynamic Host Configuration Protocol (DHCP) para atualizar o inventário de ativos corporativos** Use o log do DHCP em todos os servidores DHCP ou ferramentas de gestão de endereço Internet Protocol (IP) para atualizar o inventário de ativos corporativos. Revise e use logs para atualizar o inventário de ativos corporativos semanalmente ou com mais frequência.	Dispositivo	Identificar		●	●
1.5	**Usar uma ferramenta de descoberta passiva** Use uma ferramenta de descoberta passiva para identificar ativos conectados à rede corporativa. Revise e use varreduras para atualizar o inventário de ativos corporativos pelo menos semanalmente ou com mais frequência.	Dispositivo	Detectar			●

CONTROLE 02

Inventário e controle de ativos de software

SAFEGUARDS TOTAL	7	IG1	3/7	IG2	6/7	IG3	7/7

Visão geral

Gestão ativa (inventariar, rastrear e corrigir) de todos os softwares (sistemas operacionais e aplicações) na rede para que apenas o software autorizado seja instalado e possa ser executado, e que o software não autorizado e não gerenciado seja encontrado e impedido de ser instalado ou executado.

Por que este controle é crítico?

Um inventário de software completo é um fundamento crítico para prevenir ataques. Os atacantes realizam varreduras nas empresas continuamente em busca de versões vulneráveis de software que podem ser exploradas remotamente. Por exemplo, se um usuário abre um site malicioso ou um anexo com um navegador vulnerável, um atacante pode instalar programas backdoor e bots que fornecem ao atacante o controle de longo prazo do sistema. Os atacantes também podem usar esse acesso para mover-se lateralmente pela rede. Uma das principais defesas contra esses ataques é a atualização e a correção de software. No entanto, sem um inventário completo dos ativos de software, uma empresa não pode determinar se possui software vulnerável ou se há violações de licenciamento em potencial.

Mesmo se um patch ainda não estiver disponível, uma lista completa de inventário de software permite que uma empresa se proteja contra os ataques conhecidos até que o patch seja lançado. Alguns atacantes sofisticados usam exploits "zero-day", que tiram proveito de vulnerabilidades anteriormente desconhecidas que ainda não tiveram um patch lançado pelo fornecedor do software. Dependendo da gravidade da exploração, uma empresa pode implementar medidas de mitigação temporárias para se proteger contra ataques até que o patch seja lançado.

A gestão de ativos de software também é importante para identificar riscos de segurança desnecessários. Uma empresa deve revisar seu inventário de software para identificar quaisquer ativos corporativos executando software que não sejam necessários para fins comerciais. Por exemplo, um ativo corporativo pode vir instalado com software padrão que cria um risco potencial de segurança e não oferece nenhum benefício para a empresa. É fundamental inventariar, compreender, avaliar e gerenciar todos os softwares conectados à infraestrutura corporativa.

Procedimentos e Ferramentas

Uma lista de permissões pode ser implementada usando uma combinação de ferramentas comerciais de lista de permissões, políticas ou ferramentas de execução de aplicações que vêm com pacotes anti-malware e sistemas operacionais conhecidos. As ferramentas de inventário de software de mercado estão amplamente disponíveis e são usadas atualmente em muitas empresas. As melhores dessas ferramentas fornecem uma verificação de inventário de centenas de softwares populares usados nas empresas. As ferramentas obtêm informações sobre o nível de patch de cada programa instalado para garantir que seja a versão mais recente e aproveita nomes de aplicações padronizadas, como aqueles encontrados na especificação Common Platform Enumeration (CPE). Um exemplo de método que pode ser usado é o protocolo SCAP (Security Content Automation Protocol). Informações adicionais sobre SCAP podem ser encontradas em: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST. SP.800-126r3.pdf

Os recursos que implementam lista de permissões estão incluídos em muitos pacotes de segurança de endpoint modernos e até mesmo implementados nativamente em certas versões dos principais sistemas operacionais. Além disso, as soluções de mercado estão cada vez mais agregando antimalware, antispyware, firewall pessoal e IDS e Intrusion Prevention System (IPS) baseados em host, junto com a lista de permissões e bloqueios de aplicações. Em particular, a maioria das soluções de segurança de endpoint pode olhar para o nome, localização do sistema de arquivos e/ou hash criptográfico de um determinado executável para determinar se a aplicação deve ter permissão para ser executada na máquina protegida. As mais eficazes dessas ferramentas oferecem lista de permissões personalizada com base no caminho do executável, hash ou correspondência de expressão regular. Alguns até incluem uma função de aplicações não maliciosa, mas não aprovada, que permite aos administradores definir regras para execução de software específico para determinados usuários e em determinados horários do dia.

- **Para obter orientações específicas sobre nuvem, consulte o CIS Controls Cloud Companion Guia:** https://www.cisecurity.org/controls/v8/

- **Para obter orientação sobre tablet e smartphone, consulte o CIS Controls Mobile Companion Guia:** https://www.cisecurity.org/controls/v8/

- **Para obter orientação sobre IoT, consulte o CIS Controls Internet of Things Companion Guia:** https://www.cisecurity.org/controls/v8/

- **Para orientação de Sistemas de Controle Industrial (ICS), consulte o CIS Controls ICS Guia de implementação:** https://www.cisecurity.org/controls/v8/

Medidas de Segurança

MEDIDAS DE SEGURANÇA	TÍTULO DA MEDIDA DE SEGURANÇA/ DESCRIÇÃO DA MEDIDA DE SEGURANÇA	TIPO DE ATIVO	FUNÇÃO DE SEGURANÇA	IG1	IG2	IG3
2.1	**Estabelecer e manter um inventário de software** Estabeleça e mantenha um inventário detalhado de todos os softwares licenciados instalados em ativos corporativos. O inventário de software deve documentar o título, editor, data inicial de instalação/uso e objetivo de negócio de cada entrada; quando apropriado, inclua o Uniform Resource Locator(URL), app store(s), versão(ões), mecanismo de implantação e data de desativação. Revise e atualize o inventário de software semestralmente ou com mais frequência.	Aplicações	Identificar	●	●	●
2.2	**Assegurar que o software autorizado seja atualmente suportado** Assegure que apenas software atualmente suportado seja designado como autorizado no inventário de software para ativos corporativos. Se o software não é suportado, mas é necessário para o cumprimento da missão da empresa, documente uma exceção detalhando os controles de mitigação e a aceitação do risco residual. Para qualquer software não suportado sem uma documentação de exceção, designe como não autorizado. Revise o inventário de software para verificar o suporte do software pelo menos uma vez por mês ou com mais frequência.	Aplicações	Identificar	●	●	●
2.3	**Endereçar o software não autorizado** Assegure que o software não autorizado seja retirado de uso em ativos corporativos ou receba uma exceção documentada. Revise mensalmente ou com mais frequência	Aplicações	Responder	●	●	●
2.4	**Utilizar ferramentas automatizadas de inventário de software** Utilize ferramentas de inventário de software, quando possível, em toda a empresa para automatizar a descoberta e documentação do software instalado	Aplicações	Detectar		●	●
2.5	**Lista de permissões de Software autorizado** Use controles técnicos, como a lista de permissões de aplicações, para garantir que apenas o software autorizado possa ser executado ou acessado. Reavalie semestralmente ou com mais frequência.	Aplicações	Proteger		●	●
2.6	**Lista de permissões de bibliotecas autorizadas** Use os controles técnicos para garantir que apenas as bibliotecas de software autorizadas, como arquivos .dll, .ocx, .so, etc. específicos, tenham permissão para carregar em um processo do sistema. Impedir que bibliotecas não autorizadas sejam carregadas em um processo do sistema. Reavalie semestralmente ou com mais frequência.	Aplicações	Proteger		●	●
2.7	**Lista de permissões de Scripts autorizados** Use controles técnicos, como assinaturas digitais e controle de versão, para garantir que apenas scripts autorizados, como arquivos .ps1, .py, etc. específicos, tenham permissão para executar. Bloqueie a execução de scripts não autorizados. Reavalie semestralmente ou com mais frequência.	Aplicações	Proteger			●

CONTROLE 03

Proteção de dados

SAFEGUARDS TOTAL 14 | IG1 6/14 | IG2 12/14 | IG3 14/14

Visão geral

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

Por que este controle é crítico?

Os dados não estão mais apenas dentro da fronteira de uma empresa; estão na nuvem, em dispositivos portáteis de usuário final, onde os usuários trabalham em casa, e geralmente são compartilhados com parceiros ou serviços online que podem tê-los em qualquer lugar do mundo. Além dos dados sensíveis que uma empresa possui relacionados às finanças, propriedade intelectual e dados do cliente, também pode haver várias regulamentações internacionais para a proteção de dados pessoais. A privacidade de dados tornou-se cada vez mais importante e as empresas estão aprendendo que a privacidade diz respeito ao uso e gestão apropriados de dados, não apenas à criptografia. Os dados devem ser gerenciados de maneira adequada em todo o seu ciclo de vida. Essas regras de privacidade podem ser complicadas para empresas multinacionais de qualquer tamanho; no entanto, existem fundamentos que podem ser aplicados a todas.

Depois que os atacantes penetram na infraestrutura corporativa, uma de suas primeiras tarefas é encontrar e extrair os dados. As empresas podem não estar cientes de que dados sensíveis estão deixando seu ambiente porque não estão monitorando os fluxos de saída de dados.

Embora muitos ataques ocorram na rede, outros envolvem roubo físico de dispositivos portáteis de usuário final, ataques a provedores de serviços ou de outros parceiros que mantêm dados sensíveis. Outros ativos corporativos sensíveis também podem incluir dispositivos não computacionais que fornecem gestão e controle de sistemas físicos, como Supervisory Control and Data Acquisition (SCADA).

A perda de controle da empresa sobre os dados protegidos ou sensíveis é um sério e frequentemente relatável impacto no negócio. Embora alguns dados sejam comprometidos ou perdidos como resultado de roubo ou espionagem, a grande maioria é resultado de regras de gestão de dados mal compreendidas e de erros do usuário. A adoção da criptografia de dados, tanto em trânsito quanto em repouso, pode fornecer mitigação contra o comprometimento dos dados e, ainda mais importante, é um requisito regulatório para a maioria dos dados controlados.

Procedimentos e ferramentas

É importante para uma empresa desenvolver um processo de gestão de dados que inclua um framework de gestão de dados, diretrizes de classificação de dados e requisitos para proteção, manuseio, retenção e descarte de dados. Também deve haver um processo de violação de dados que se conecte ao plano de resposta a incidentes e aos planos de conformidade e comunicação. Para obter os níveis de sensibilidade dos dados, as empresas precisam catalogar seus principais tipos de dados e a criticidade geral (impacto para sua perda ou corrupção) para a empresa. Essa análise deveria ser usada para criar um esquema geral de classificação de dados para a empresa. As empresas podem usar rótulos, como "Sensível", "Confidencial" e "Público", e classificar seus dados de acordo com esses rótulos.

Uma vez que a sensibilidade dos dados tenha sido definida, um inventário ou mapeamento de dados deve ser desenvolvido para identificar o software que acessa os dados em vários níveis de sensibilidade e os ativos corporativos que hospedam essas aplicações. Idealmente, a rede deveria ser separada para que os ativos corporativos do mesmo nível de sensibilidade estejam na mesma rede e separados dos ativos corporativos com diferentes níveis de sensibilidade. Se possível, os firewalls precisam controlar o acesso a cada segmento e ter regras de acesso de usuário aplicadas para permitir que apenas aqueles com necessidade de negócios acessem estes dados.

Para um tratamento mais abrangente deste tópico, sugerimos os seguintes recursos para ajudar a empresa com a proteção de dados:

- **NIST® SP 800-88r1 Guides for Media Sanitization:** https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf
- **NIST® FIPS 140-2:**https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf
- **NIST® FIPS 140-3:**https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf
- **Para obter orientação específica sobre nuvem, consulte o CIS Controls Cloud Companion Guide:** https://www.cisecurity.org/controls/v8/
- **Para obter orientação sobre tablet e smartphone, consulte o CIS Controls Mobile Companion Guide:** https://www.cisecurity.org/controls/v8/

Medidas de Segurança

MEDIDAS DE SEGURANÇA	TÍTULO DA MEDIDA DE SEGURANÇA/ DESCRIÇÃO DA MEDIDA DE SEGURANÇA	TIPO DE ATIVO	FUNÇÃO DE SEGURANÇA	IG1	IG2	IG3
3.1	**Estabelecer e manter um processo de gestão de dados** Estabeleça e mantenha um processo de gestão de dados. No processo, trate a sensibilidade dos dados, o proprietário dos dados, o manuseio dos dados, os limites de retenção de dados e os requisitos de descarte, com base em padrões de sensibilidade e retenção para a empresa. Revise e atualize a documentação anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.	Dados	Identificar	●	●	●
3.2	**Estabelecer e manter um inventário de dados** Estabeleça e mantenha um inventário de dados, com base no processo de gestão de dados da empresa. No mínimo, inventarie os dados sensíveis. Revise e atualize o inventário anualmente, no mínimo, com prioridade para os dados sensíveis.	Dados	Identificar	●	●	●

MEDIDAS DE SEGURANÇA	TÍTULO DA MEDIDA DE SEGURANÇA/ DESCRIÇÃO DA MEDIDA DE SEGURANÇA	TIPO DE ATIVO	FUNÇÃO DE SEGURANÇA	IG1	IG2	IG3
3.3	**Configurar listas de controle de acesso a dados** Configure listas de controle de acesso a dados com base na necessidade de conhecimento do usuário. Aplique listas de controle de acesso a dados, também conhecidas como permissões de acesso, a sistemas de arquivos, bancos de dados e aplicações locais e remotos.	Dados	Proteger	●	●	●
3.4	**Aplicar retenção de dados** Retenha os dados de acordo com o processo de gestão de dados da empresa. A retenção de dados deve incluir prazos mínimos e máximos.	Dados	Proteger	●	●	●
3.5	**Descartar dados com segurança** Descarte os dados com segurança conforme descrito no processo de gestão de dados da empresa. Certifique-se de que o processo e o método de descarte sejam compatíveis com a sensibilidade dos dados.	Dados	Proteger	●	●	●
3.6	**Criptografar dados em dispositivos de usuário final.** Criptografe os dados em dispositivos de usuário final que contenham dados sensíveis. Exemplos de implementações podem incluir: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.	Dispositivo	Proteger	●	●	●
3.7	**Estabelecer e manter um esquema de classificação de dados** Estabeleça e mantenha um esquema geral de classificação de dados para a empresa. As empresas podem usar rótulos, como "Sensível", "Confidencial" e "Público", e classificar seus dados de acordo com esses rótulos. Revise e atualize o esquema de classificação anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.	Dados	Identificar		●	●
3.8	**Documentar Fluxos de Dados** Documente fluxos de dados. A documentação do fluxo de dados inclui fluxos de dados do provedor de serviços e deve ser baseada no processo de gestão de dados da empresa. Revise e atualize a documentação anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança	Dados	Identificar		●	●
3.9	**Criptografar dados em mídia removível** Criptografe os dados em mídia removível.	Dados	Proteger		●	●
3.10	**Criptografar dados sensíveis em trânsito** Criptografe dados sensíveis em trânsito. Exemplos de implementações podem incluir: Transport Layer Security (TLS) e Open Secure Shell (OpenSSH)	Dados	Proteger		●	●
3.11	**Criptografar dados sensíveis em repouso** Criptografe dados sensíveis em repouso em servidores, aplicações e bancos de dados que contenham dados sensíveis. A criptografia da camada de armazenamento, também conhecida como criptografia do lado do servidor, atende ao requisito mínimo desta medida de segurança. Métodos de criptografia adicionais podem incluir criptografia de camada de aplicação, também conhecida como criptografia do lado do cliente, onde o acesso ao(s) dispositivo(s) de armazenamento de dados não permite o acesso aos dados em texto simples.	Dados	Proteger		●	●
3.12	**Segmentar o processamento e o armazenamento de dados com base na sensibilidade** Segmente o processamento e o armazenamento de dados com base na sensibilidade dos dados. Não processe dados sensíveis em ativos corporativos destinados a dados de menor sensibilidade.	Rede	Proteger		●	●
3.13	**Implantar uma solução de prevenção contra perda de dados** Implementar uma ferramenta automatizada, como uma ferramenta de prevenção de perda de dados (DLP) baseada em host para identificar todos os dados sensíveis armazenados, processados ou transmitidos por meio de ativos corporativos, incluindo aqueles localizados no site local ou em um provedor de serviços remoto, e atualizar o inventário de dados sensíveis da empresa.	Dados	Proteger			●
3.14	**Registrar o acesso a dados sensíveis** Registre o acesso a dados sensíveis, incluindo modificação e descarte.	Dados	Detectar			●

CONTROLE 04

Configuração segura de ativos corporativos e software

SAFEGUARDS TOTAL 12 | IG1 7/12 | IG2 11/12 | IG3 12/12

Visão geral

Estabelecer e manter a configuração segura de ativos corporativos (dispositivos de usuário final, incluindo portáteis e móveis; dispositivos de rede; dispositivos não computacionais/IoT; e servidores) e software (sistemas operacionais e aplicações).

Por que este controle é crítico?

Conforme fornecidas pelos fabricantes e revendedores, as configurações padrão para ativos e software corporativos são normalmente voltadas para a facilidade de implantação e uso, em vez da segurança. Controles básicos, serviços e portas abertos, contas ou senhas padrão, definições pré-configuradas de Domain Name System (DNS), protocolos mais antigos (vulneráveis) e pré-instalação de software desnecessário podem ser explorados se deixados em seu estado padrão. Além disso, essas atualizações de configuração de segurança precisam ser gerenciadas e mantidas ao longo do ciclo de vida dos ativos e software da empresa. As atualizações de configuração precisam ser rastreadas e aprovadas por meio de um processo de fluxo de trabalho de gestão de configuração para manter um registro que pode ser revisado para compliance, aproveitado para resposta a incidentes e para apoiar auditorias. Este controle CIS é importante para dispositivos locais, bem como dispositivos remotos, dispositivos de rede e ambientes de nuvem.

Os provedores de serviços desempenham um papel fundamental nas infraestruturas modernas, especialmente para empresas menores. Elas geralmente não são definidas por padrão na configuração mais segura de forma a fornecer flexibilidade para que seus clientes apliquem suas próprias políticas de segurança. Portanto, a presença de contas ou senhas padrão, acesso excessivo ou serviços desnecessários são comuns nas configurações padrão. Isso pode introduzir fraquezas que são de responsabilidade da empresa que está usando o software, e não do provedor de serviços. Isso se estende à gestão e atualizações contínuas, já que algumas Platform as a Service (PaaS) se estendem apenas ao sistema operacional, portanto, a aplicação de patches e a atualização de aplicações hospedadas são de responsabilidade da empresa.

Mesmo depois que uma configuração inicial forte é desenvolvida e aplicada, ela deve ser gerenciada continuamente para evitar a degradação da segurança à medida que o software é atualizado ou corrigido, novas vulnerabilidades de segurança são relatadas e as configurações são "ajustadas" para permitir a instalação de um novo software ou para oferecer suporte para novos requisitos operacionais.

Procedimentos e ferramentas

Existem muitos baselines de segurança disponíveis para cada sistema. As empresas devem começar com esses benchmarks de segurança, guias de segurança ou checklists publicamente desenvolvidos, verificados e suportados. Alguns recursos incluem:

- **The CIS Benchmarks™ Program:** http://www.cisecurity.org/cis-benchmarks/
- **The National Institute of Standards and Technology (NIST®) National Checklist Program Repository:** https://nvd.nist.gov/ncp/repository

As empresas devem ampliar ou ajustar esses baselines para atender às políticas de segurança corporativas e aos requisitos regulatórios do setor e do governo. Desvios de configurações padrão e justificativas devem ser documentados para facilitar futuras revisões ou auditorias.

Para uma empresa maior ou mais complexa, haverá várias configurações de baseline de segurança com base nos requisitos de segurança ou classificação dos dados no ativo corporativo. Aqui está um exemplo das etapas para construir uma imagem de baseline segura:

01 Determine a classificação de risco dos dados manipulados/armazenados no ativo corporativo (por exemplo, risco alto, moderado, baixo).

02 Crie um script de configuração de segurança que defina as configurações de segurança do sistema para atender aos requisitos para proteger os dados usados no ativo corporativo. Use benchmarks, como os descritos anteriormente nesta seção.

03 Instale o software básico do sistema operacional.

04 Aplique o sistema operacional e os patches de segurança apropriados.

05 Instale os pacotes, ferramentas e utilitários de software de aplicação apropriados.

06 Aplique as atualizações apropriadas ao software instalado na Etapa 4.

07 Instale scripts de customização locais nesta imagem.

08 Execute o script de segurança criado na Etapa 2 para definir o nível de segurança apropriado.

09 Execute uma ferramenta compatível com o SCAP para registrar/pontuar a configuração do sistema da imagem do baseline.

10 Execute um teste de garantia de qualidade de segurança.

11 Salve esta imagem de base em um local seguro.

Ferramentas de mercado e/ou gratuitas de gestão de configuração, como a CIS Configuration Assessment Tool (CIS-CAT®) https://learn.cisecurity.org/cis-cat-lite, podem ser implantadas para medir as configurações de sistemas operacionais e aplicações de máquinas gerenciadas para procurar desvios das configurações da imagem padrão. As ferramentas de gestão de configuração de mercado usam alguma combinação de um agente instalado em cada sistema gerenciado ou inspeção sem agente de sistemas por meio de login remoto em cada ativo corporativo usando credenciais de administrador. Além disso, às vezes é usada uma abordagem híbrida por meio da qual uma sessão remota é iniciada, um agente temporário ou dinâmico é implementado no sistema de destino para a varredura e, em seguida, o agente é removido.

Medidas de Segurança

MEDIDAS DE SEGURANÇA	TÍTULO DA MEDIDA DE SEGURANÇA/ DESCRIÇÃO DA MEDIDA DE SEGURANÇA	TIPO DE ATIVO	FUNÇÃO DE SEGURANÇA	IG1	IG2	IG3
4.1	**Estabelecer e manter um processo de configuração segura** Estabeleça e mantenha um processo de configuração segura para ativos corporativos (dispositivos de usuário final, incluindo portáteis e móveis; dispositivos não computacionais/IoT; e servidores) e software (sistemas operacionais e aplicações). Revise e atualize a documentação anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.	Aplicações	Proteger	●	●	●
4.2	**Estabelecer e Manter um Processo de Configuração Segura para a Infraestrutura de Rede** Estabeleça e mantenha um processo de configuração segura para dispositivos de rede. Revise e atualize a documentação anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.	Rede	Proteger	●	●	●
4.3	**Configurar o bloqueio automático de sessão nos ativos corporativos** Configure o bloqueio automático de sessão nos ativos corporativos após um período definido de inatividade. Para sistemas operacionais de uso geral, o período não deve exceder 15 minutos. Para dispositivos móveis de usuário final, o período não deve exceder 2 minutos.	Usuários	Proteger	●	●	●
4.4	**Implementar e gerenciar um firewall nos servidores** Implemente e gerencie um firewall nos servidores, onde houver suporte. Exemplos de implementações incluem um firewall virtual, firewall do sistema operacional ou um agente de firewall de terceiros.	Dispositivo	Proteger	●	●	●
4.5	**Implementar e gerenciar um firewall nos dispositivos de usuário final** Implemente e gerencie um firewall baseado em host ou uma ferramenta de filtragem de porta nos dispositivos de usuário final, com uma regra de negação padrão que bloqueia todo o tráfego, exceto os serviços e portas que são explicitamente permitidos.	Dispositivo	Proteger	●	●	●
4.6	**Gerenciar com segurança os ativos e software corporativos** Gerencie com segurança os ativos e software corporativos. Exemplos de implementações incluem gestão de configuração por meio de version-controlled-infrastructure-as-code e acesso a interfaces administrativas por meio de protocolos de rede seguros, como Secure Shell (SSH) e Hypertext Transfer Protocol Secure (HTTPS). Não use protocolos de gestão inseguros, como Telnet (Teletype Network) e HTTP, a menos que seja operacionalmente essencial.	Rede	Proteger	●	●	●
4.7	**Gerenciar contas padrão nos ativos e software corporativos** Gerencie contas padrão nos ativos e software corporativos, como root, administrador e outras contas de fornecedores pré-configuradas. Exemplos de implementações podem incluir: desativar contas padrão ou torná-las inutilizáveis.	Usuários	Proteger	●	●	●
4.8	**Desinstalar ou desativar serviços desnecessários nos ativos e software corporativos** Desinstale ou desative serviços desnecessários nos ativos e software corporativos, como um serviço de compartilhamento de arquivos não utilizado, módulo de aplicação da web ou função de serviço.	Dispositivo	Proteger		●	●
4.9	**Configurar servidores DNS confiáveis nos ativos corporativos** Configure servidores DNS confiáveis nos ativos corporativos. As exemplos de implementações incluem: configuração de ativos para usar servidores DNS controlados pela empresa e/ou servidores DNS confiáveis acessíveis externamente.	Dispositivo	Proteger		●	●

MEDIDAS DE SEGURANÇA	TÍTULO DA MEDIDA DE SEGURANÇA/ DESCRIÇÃO DA MEDIDA DE SEGURANÇA	TIPO DE ATIVO	FUNÇÃO DE SEGURANÇA	IG1	IG2	IG3
4.10	**Impor o bloqueio automático de dispositivos nos dispositivos portáteis do usuário final** Imponha o bloqueio automático do dispositivo seguindo um limite pré-determinado de tentativas de autenticação local com falha nos dispositivos portáteis de usuário final, quando compatível. Para laptops, não permita mais de 20 tentativas de autenticação com falha; para tablets e smartphones, não mais do que 10 tentativas de autenticação com falha. Exemplos de implementações incluem Microsoft® InTune Device Lock e Apple® Configuration Profile maxFailedAttempts.	Dispositivo	Responder		●	●
4.11	**Impor a capacidade de limpeza remota nos dispositivos portáteis do usuário final** Limpe remotamente os dados corporativos de dispositivos portáteis de usuário final de propriedade da empresa quando for considerado apropriado, como dispositivos perdidos ou roubados, ou quando um indivíduo não trabalha mais na empresa.	Dispositivo	Proteger		●	●
4.12	**Separar os Espaços de Trabalho Corporativos nos dispositivos móveis** Certifique-se de que a separação de espaços de trabalho corporativos seja usada nos dispositivos móveis de usuário final, onde houver suporte. Exemplos de implementações incluem o uso de um Apple® Configuration Profile ou Android ™ Work Profile para separar aplicações e dados corporativos de aplicações e dados pessoais.	Dispositivo	Proteger			●

CONTROLE 05

Gestão de contas

SAFEGUARDS TOTAL	6	IG1	4/6	IG2	6/6	IG3	6/6

Visão geral

Use processos e ferramentas para atribuir e gerenciar autorização de credenciais para contas de usuário, incluindo contas de administrador, bem como contas de serviço, de ativos corporativos e software.

Por que este controle é crítico?

É mais fácil para um agente de ameaça externo ou interno obter acesso não autorizado a ativos ou dados da empresa usando credenciais de usuário válidas do que "hackeando" o ambiente. Existem muitas maneiras de obter secretamente acesso a contas de usuário, incluindo: senhas fracas, contas ainda válidas depois que um usuário deixa a empresa, contas de teste inativas ou remanescentes, contas compartilhadas que não foram alteradas em meses ou anos, contas de serviço incorporadas em aplicações para scripts, um usuário com a mesma senha que eles usam para uma conta online que foi comprometida (em um dump de senha pública), engenharia social em um usuário para fornecer sua senha ou usar malware para capturar senhas ou tokens na memória ou na rede.

Contas administrativas ou altamente privilegiadas são um alvo específico porque permitem que atacantes adicionem outras contas ou façam alterações em ativos que podem torná-los mais vulneráveis a outros ataques. As contas de serviço também são sensíveis, pois geralmente são compartilhadas entre as equipes, internas e externas à empresa, e às vezes desconhecidas, apenas para serem reveladas em auditorias de gestão de contas padrão.

Por fim, o registro e o monitoramento de contas são componentes críticos das operações de segurança. Embora o registro e monitoramento de contas sejam cobertos pelo Controle CIS 8 (Gestão de Log de Auditoria), é importante no desenvolvimento de um programa abrangente de Gestão de Acesso e Identidades (Identity and Access Management—IAM).

Procedimentos e ferramentas

Credenciais são ativos que devem ser inventariados e rastreados semelhante a ativos e software corporativos, pois são o principal ponto de entrada na empresa. Devem ser desenvolvidas políticas de senha adequadas e orientações para não reutilizar senhas. Para obter orientação sobre a criação e uso de senhas, consulte o CIS Password Policy Guide: https://www.cisecurity.org/white-papers/cis-passwordpolicy-guide/

As contas também devem ser rastreadas; qualquer conta que esteja inativa deve ser desabilitada e eventualmente removida do sistema. Deve haver auditorias periódicas para garantir que todas as contas ativas sejam rastreadas para usuários autorizados do ativo corporativo. Procure novas contas adicionadas desde a revisão anterior, especialmente contas de administrador e de serviço. Deve-se prestar muita atenção para identificar e rastrear contas administrativas ou de alto privilégio e contas de serviço.

Os usuários com acesso de administrador ou outro acesso privilegiado devem ter contas separadas para essas tarefas de maior autoridade. Essas contas deveriam ser usadas apenas para executar essas tarefas ou acessar dados especialmente sensíveis, para reduzir o risco no caso de sua conta de usuário normal ser comprometida. Para usuários com várias contas, sua conta de usuário comum, usada diariamente para tarefas não administrativas, não deve ter nenhum privilégio elevado.

O Single Sign-On (SSO) é conveniente e seguro quando uma empresa tem muitas aplicações, incluindo aplicações em nuvem, o que ajuda a reduzir o número de senhas que um usuário deve gerenciar. Recomenda-se que os usuários usem aplicações de gestão de senhas para armazenar com segurança suas senhas e devem ser instruídos a não mantê-las em planilhas ou arquivos de texto em seus computadores. O MFA é recomendado para acesso remoto.

Os usuários também devem ser desconectados automaticamente do sistema após um período de inatividade, e ser treinados para bloquear a tela ao sair do dispositivo para minimizar a possibilidade de outra pessoa na proximidade física do usuário acessar seu sistema, aplicações ou dados.

→ **Um excelente recurso é o NIST® Digital Identity Guideline:** https://pages.nist.gov/800-63-3/

Medidas de Segurança

MEDIDAS DE SEGURANÇA	TÍTULO DA MEDIDA DE SEGURANÇA/ DESCRIÇÃO DA MEDIDA DE SEGURANÇA	TIPO DE ATIVO	FUNÇÃO DE SEGURANÇA	IG1	IG2	IG3
5.1	**Estabelecer e manter um inventário de contas** Estabeleça e mantenha um inventário de todas as contas gerenciadas na empresa. O inventário deve incluir contas de usuário e administrador. O inventário, no mínimo, deve conter o nome da pessoa, nome de usuário, datas de início/término e departamento. Valide se todas as contas ativas estão autorizadas, em uma programação recorrente, no mínimo trimestralmente ou com mais frequência.	Usuários	Identificar	●	●	●
5.2	**Usar senhas exclusivas** Use senhas exclusivas para todos os ativos corporativos. As melhores práticas de implementação incluem, no mínimo, uma senha de 8 caracteres para contas que usam MFA e uma senha de 14 caracteres para contas que não usam MFA.	Usuários	Proteger	●	●	●

MEDIDAS DE SEGURANÇA	TÍTULO DA MEDIDA DE SEGURANÇA/ DESCRIÇÃO DA MEDIDA DE SEGURANÇA	TIPO DE ATIVO	FUNÇÃO DE SEGURANÇA	IG1	IG2	IG3
5.3	**Desabilitar contas inativas** Exclua ou desabilite quaisquer contas inativas após um período de 45 dias de inatividade, onde for suportado.	Usuários	Responder	●	●	●
5.4	**Restringir privilégios de administrador a contas de Administrador dedicadas** Restrinja os privilégios de administrador a contas de administrador dedicadas nos ativos corporativos. Realize atividades gerais de computação, como navegação na Internet, e-mail e uso do pacote de produtividade, a partir da conta primária não privilegiada do usuário.	Usuários	Proteger	●	●	●
5.5	**Estabelecer e manter um inventário de contas de serviço** Estabeleça e mantenha um inventário de contas de serviço. O inventário, no mínimo, deve conter departamento proprietário, data de revisão e propósito. Realize análises de contas de serviço para validar se todas as contas ativas estão autorizadas, em uma programação recorrente, no mínimo trimestralmente ou com mais frequência.	Usuários	Identificar		●	●
5.6	**Centralizar a gestão de contas** Centralize a gestão de contas por meio de serviço de diretório ou de identidade.	Usuários	Proteger		●	●

CONTROLE 06

Gestão do controle de acesso

SAFEGUARDS TOTAL	8	IG1	5/8	IG2	7/8	IG3	8/8

Visão geral

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

Por que este controle é crítico?

Onde o Controle CIS 5 lida especificamente com a gestão de contas, o Controle CIS 6 se concentra em gerenciar o acesso dessas contas, garantindo que os usuários tenham acesso apenas aos dados ou ativos corporativos apropriados para suas funções e garantindo que haja autenticação forte para dados ou funções corporativas críticas ou sensíveis. As contas devem ter apenas a autorização mínima necessária para a função. O desenvolvimento de direitos de acesso consistentes para cada função e a atribuição de funções aos usuários é uma prática recomendada. O desenvolvimento de um programa para acesso completo e desprovisionamento também é importante. Centralizar essa função é o ideal.

Existem algumas atividades de usuário que representam um maior risco para a empresa, seja porque eles são acessados de redes não confiáveis, ou por realizar funções de administrador que permitem adicionar, alterar e remover outras contas, ou fazer alterações de configuração em sistemas operacionais e aplicações para torná-los menos seguros. Isso também reforça a importância do uso de ferramentas MFA e Privileged Access Management (PAM)

Alguns usuários têm acesso a ativos ou dados corporativos de que não precisam para sua função; isso pode ser devido a um processo imaturo que concede a todos os usuários acesso total ou acesso prolongado à medida que os usuários mudam de função dentro da empresa ao longo do tempo. Os privilégios de administrador local para os laptops dos usuários também são um problema, pois códigos maliciosos instalados ou baixados pelo usuário podem ter um impacto maior no ativo corporativo executado como administrador. O acesso de usuário, administrador e conta de serviço deve ser baseado na função e na necessidade da empresa.

Procedimentos e ferramentas

Deve haver um processo em que os privilégios são concedidos e revogados para contas de usuário. Idealmente, isso se baseia na função e na necessidade da empresa por meio do acesso baseado em função (role-based access). O acesso baseado em função é uma técnica para definir e gerenciar os requisitos de acesso para cada conta com base em: necessidade de saber, privilégio mínimo, requisitos de privacidade, e/ou separação de funções. Existem ferramentas tecnológicas para ajudar a gerenciar esse processo. No entanto, baseado nas circunstâncias pode haver acesso mais granular ou temporário.

O MFA deve ser universal para todas as contas privilegiadas ou de administrador. Existem muitas ferramentas que possuem aplicações de smartphone que executam essa função e são fáceis de implantar. Usar o recurso de geração de números é mais seguro do que apenas enviar uma mensagem SMS (Short Messaging Service) com um código único ou solicitar um alerta "push" para o usuário aceitar. No entanto, nenhum dos dois é recomendado para MFA de conta privilegiada. As ferramentas PAM estão disponíveis para controle de conta com privilégios e fornecem uma senha de uso único que deve ser verificada para cada uso. Para segurança adicional na administração do sistema, o uso de "jump boxes" ou conexões de terminal fora de banda é recomendado.

O desprovisionamento abrangente de contas é importante. Muitas empresas têm processos consistentes que podem ser repetidos para remover o acesso quando os funcionários deixam a empresa. No entanto, esse processo nem sempre é consistente para os contratados e deve ser incluído no processo de desprovisionamento padrão. As empresas também devem inventariar e rastrear contas de serviço, pois um erro comum é deixar tokens e senhas em texto claro no código e postar em repositórios de código em nuvem pública.

Contas de alto privilégio não devem ser usadas para uso diário, como navegação na web e leitura de e-mail. Os administradores devem ter contas separadas que não tenham privilégios elevados para uso diário no escritório e devem fazer login em contas de administrador apenas quando executarem funções de administrador que requeiram esse nível de autorização. A equipe de segurança deve reunir periodicamente uma lista de processos em execução para determinar se algum navegador ou leitor de e-mail está executando com altos privilégios.

→ **Um excelente recurso é o NIST® Digital Identity Guidelines:** https://pages.nist.gov/800-63-3/

Medidas de Segurança

MEDIDAS DE SEGURANÇA	TÍTULO DA MEDIDA DE SEGURANÇA/ DESCRIÇÃO DA MEDIDA DE SEGURANÇA	TIPO DE ATIVO	FUNÇÃO DE SEGURANÇA	IG1	IG2	IG3
6.1	**Estabelecer um Processo de Concessão de Acesso** Estabeleça e siga um processo, de preferência automatizado, para conceder acesso aos ativos corporativos mediante nova contratação, concessão de direitos ou mudança de função de um usuário.	Usuários	Proteger	●	●	●
6.2	**Estabelecer um Processo de Revogação de Acesso** Estabeleça e siga um processo, de preferência automatizado, para revogar o acesso aos ativos corporativos, por meio da desativação de contas imediatamente após o encerramento, revogação de direitos ou mudança de função de um usuário. Desativar contas, em vez de excluí-las, pode ser necessário para preservar as trilhas de auditoria.	Usuários	Proteger	●	●	●

MEDIDAS DE SEGURANÇA	TÍTULO DA MEDIDA DE SEGURANÇA/ DESCRIÇÃO DA MEDIDA DE SEGURANÇA	TIPO DE ATIVO	FUNÇÃO DE SEGURANÇA	IG1	IG2	IG3
6.3	**Exigir MFA para aplicações expostas externamente** Exija que todas as aplicações corporativas ou de terceiros expostas externamente apliquem o MFA, onde houver suporte. Impor o MFA por meio de um serviço de diretório ou provedor de SSO é uma implementação satisfatória desta medida de segurança	Usuários	Proteger	●	●	●
6.4	**Exigir MFA para acesso remoto à rede** Exija MFA para acesso remoto à rede.	Usuários	Proteger	●	●	●
6.5	**Exigir MFA para acesso administrativo** Exija MFA para todas as contas de acesso administrativo, onde houver suporte, em todos os ativos corporativos, sejam gerenciados no site local ou por meio de um provedor terceirizado.	Usuários	Proteger	●	●	●
6.6	**Estabelecer e manter um inventário de sistemas de autenticação e autorização** Estabeleça e mantenha um inventário dos sistemas de autenticação e autorização da empresa, incluindo aqueles hospedados no site local ou em um provedor de serviços remoto. Revise e atualize o inventário, no mínimo, anualmente ou com mais frequência.	Usuários	Identificar		●	●
6.7	**Centralizar o controle de acesso** Centralize o controle de acesso para todos os ativos corporativos por meio de um serviço de diretório ou provedor de SSO, onde houver suporte.	Usuários	Proteger		●	●
6.8	**Definir e manter o controle de acesso baseado em funções** Defina e mantenha o controle de acesso baseado em funções, determinando e documentando os direitos de acesso necessários para cada função dentro da empresa para cumprir com sucesso suas funções atribuídas. Realize análises de controle de acesso de ativos corporativos para validar se todos os privilégios estão autorizados, em uma programação recorrente, no mínimo uma vez por ano ou com maior frequência.	Dados	Proteger			●

CONTROLE 07

Gestão contínua de vulnerabilidades

SAFEGUARDS TOTAL	7	IG1	4/7	IG2	7/7	IG3	7/7

Visão geral

Desenvolva um plano para avaliar e rastrear vulnerabilidades continuamente em todos os ativos corporativos dentro da infraestrutura da empresa, a fim de remediar e minimizar a janela de oportunidade para atacantes. Monitore fontes públicas e privadas para novas informações sobre ameaças e vulnerabilidades.

Por que este controle é crítico?

Os defensores cibernéticos são constantemente desafiados por atacantes que procuram vulnerabilidades em sua infraestrutura para explorar e obter acesso. Os defensores devem ter informações oportunas de ameaças disponíveis sobre: atualizações de software, patches, avisos de segurança, boletins de ameaças, etc., e devem revisar regularmente seu ambiente para identificar essas vulnerabilidades antes que os atacantes o façam. Compreender e gerenciar vulnerabilidades é uma atividade contínua, que requer foco de tempo, atenção e recursos.

Os atacantes têm acesso às mesmas informações e muitas vezes podem tirar proveito das vulnerabilidades mais rapidamente do que uma empresa pode remediar. Embora exista um intervalo de tempo desde a descoberta de uma vulnerabilidade até quando ela é corrigida, os defensores podem priorizar quais vulnerabilidades são mais impactantes para a empresa ou que provavelmente serão exploradas primeiro devido à facilidade de uso. Por exemplo, quando os pesquisadores ou a comunidade relatam novas vulnerabilidades, os fornecedores precisam desenvolver e implantar patches, indicadores de comprometimento (IOCs) e atualizações. Os defensores precisam avaliar o risco da nova vulnerabilidade para a empresa, realizar testes de regressão nos patches e instalar o patch.

Nunca há perfeição neste processo. Os atacantes podem estar usando um exploit para uma vulnerabilidade que não é conhecida na comunidade de segurança. Eles podem ter desenvolvido um exploit para essa vulnerabilidade, conhecido como exploit de "zero-day". Uma vez que a vulnerabilidade é conhecida na comunidade, o processo mencionado acima é iniciado. Portanto, os defensores devem ter em mente que pode já existir um exploit quando a vulnerabilidade é amplamente socializada. Às vezes, as vulnerabilidades podem ser conhecidas em uma comunidade fechada (por exemplo, o fornecedor ainda está desenvolvendo uma correção) por semanas, meses ou anos antes de serem divulgadas publicamente. Os defensores devem estar cientes de que pode sempre haver vulnerabilidades que eles não podem remediar e, portanto, precisam usar outros controles para mitigar.

As empresas que não avaliam sua infraestrutura em busca de vulnerabilidades e corrigem prontamente as falhas descobertas possuem uma probabilidade significativa de ter seus ativos corporativos comprometidos. Os defensores enfrentam desafios específicos ao dimensionar a remediação em toda a empresa e priorizar ações com prioridades conflitantes, para que não afetem os negócios ou a missão da empresa.

Procedimentos e ferramentas

Um grande número de ferramentas de varredura de vulnerabilidade está disponível para avaliar a configuração de segurança de ativos corporativos. Algumas empresas também descobriram que os serviços comerciais que usam dispositivos de varredura gerenciados remotamente são eficazes. Para ajudar a padronizar as definições de vulnerabilidades descobertas em uma empresa, é preferível usar ferramentas de varredura de vulnerabilidades que mapeiam vulnerabilidades para uma ou mais das seguintes vulnerabilidades, esquemas de configuração e classificação de plataforma e linguagens reconhecidos pela indústria: Common Vulnerabilities and Exposuress (CVE®), Common Configuration Enumeration (CCE), Open Vulnerability and Assessment Language (OVAL®), Common Platform Enumeration (CPE), Common Vulnerability Scoring System (CVSS) e/ou Extensible Configuration Checklist Description Format (XCCDF).

→ **Mais informações sobre SCAP podem ser encontradas aqui:** https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-126r3.pdf

A frequência das atividades de varredura deve aumentar à medida que a diversidade dos ativos de uma empresa aumenta levando em conta os ciclos de patch variáveis de cada fornecedor. Ferramentas avançadas de varredura de vulnerabilidade podem ser configuradas com credenciais de usuário para autenticação em ativos corporativos e realização de avaliações mais abrangentes. Eles são chamados de "varreduras autenticadas".

Além das ferramentas de varredura que verificam vulnerabilidades e configurações incorretas na rede, várias ferramentas gratuitas e comerciais podem avaliar as configurações de segurança e configurações de ativos corporativos. Essas ferramentas podem fornecer uma visão detalhada das alterações não autorizadas na configuração ou da introdução inadvertida de falhas de segurança por parte dos administradores.

Empresas eficazes vinculam seus scanners de vulnerabilidade a sistemas de tíquetes de problemas que rastreiam e relatam o progresso na correção de vulnerabilidades. Isso pode ajudar a destacar vulnerabilidades críticas não mitigadas para a alta administração de forma a garantir que sejam resolvidas. As empresas também podem rastrear quanto tempo levou para corrigir uma vulnerabilidade, depois de identificada, ou de um patch ter sido lançado. Eles podem oferecer suporte a requisitos de conformidade internos ou do setor. Algumas empresas maduras examinarão esses relatórios em reuniões do comitê de segurança de TI, que reúnem líderes de TI e de negócios para priorizar os esforços de remediação com base no impacto nos negócios.

Ao selecionar quais vulnerabilidades corrigir ou patches aplicar, uma empresa deve acrescentar o Common Vulnerability Scoring System (CVSS) do NIST com dados sobre a probabilidade de um agente de ameaça usar uma vulnerabilidade ou potencial impacto de uma exploração na empresa. As informações sobre a probabilidade de exploração também devem ser atualizadas periodicamente com base nas informações mais recentes sobre ameaças. Por exemplo, o lançamento de um novo exploit ou nova inteligência relacionada à exploração da vulnerabilidade deve mudar a prioridade pela qual a vulnerabilidade deve ser considerada para correção. Vários sistemas comerciais estão disponíveis para permitir que uma empresa automatize e mantenha esse processo de maneira escalável.

As ferramentas de varredura de vulnerabilidade mais eficazes comparam os resultados da varredura atual com varreduras anteriores para determinar como as vulnerabilidades no ambiente mudaram ao longo do tempo. O pessoal de segurança usa esses recursos para avaliar a tendência de vulnerabilidades mês a mês.

Finalmente, deve haver um processo de garantia de qualidade para verificar as atualizações de configuração, ou que os patches são implementados corretamente e em todos os ativos empresariais relevantes.

Medidas de Segurança

MEDIDAS DE SEGURANÇA	TÍTULO DA MEDIDA DE SEGURANÇA/ DESCRIÇÃO DA MEDIDA DE SEGURANÇA	TIPO DE ATIVO	FUNÇÃO DE SEGURANÇA	IG1	IG2	IG3
7.1	**Estabelecer e manter um processo de gestão de vulnerabilidade** Estabeleça e mantenha um processo de gestão de vulnerabilidade documentado para ativos corporativos. Revise e atualize a documentação anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.	Aplicações	Proteger	●	●	●
7.2	**Estabelecer e manter um processo de remediação** Estabeleça e mantenha uma estratégia de remediação baseada em risco documentada em um processo de remediação, com revisões mensais ou mais frequentes.	Aplicações	Responder	●	●	●
7.3	**Executar a gestão automatizada de patches do sistema operacional** Realize atualizações do sistema operacional em ativos corporativos por meio da gestão automatizada de patches mensalmente ou com mais frequência.	Aplicações	Proteger	●	●	●
7.4	**Executar a gestão automatizada de patches de aplicações** Realize atualizações de aplicações em ativos corporativos por meio da gestão automatizada de patches mensalmente ou com mais frequência.	Aplicações	Proteger	●	●	●
7.5	**Realizar varreduras automatizadas de vulnerabilidade em ativos corporativos internos** Realize varreduras automatizadas de vulnerabilidade em ativos corporativos internos trimestralmente ou com mais frequência. Realize varreduras autenticadas e não autenticadas, usando uma ferramenta de varredura de vulnerabilidade compatível com o SCAP.	Aplicações	Identificar		●	●
7.6	**Realizar varreduras automatizadas de vulnerabilidade em ativos corporativos expostos externamente** Execute varreduras de vulnerabilidade automatizadas de ativos corporativos expostos externamente usando uma ferramenta de varredura de vulnerabilidade compatível com o SCAP. Execute varreduras mensalmente ou com mais frequência.	Aplicações	Identificar		●	●
7.7	**Corrigir vulnerabilidades detectadas** Corrija as vulnerabilidades detectadas no software por meio de processos e ferramentas mensalmente, ou mais frequentemente, com base no processo de correção.	Aplicações	Responder		●	●

CONTROLE 08

Gestão de registros de auditoria

SAFEGUARDS TOTAL 12 | IG1 3/12 | IG2 11/12 | IG3 12/12

Visão geral

Colete, alerte, analise e retenha logs de auditoria de eventos que podem ajudar a detectar, compreender ou se recuperar de um ataque.

Por que este controle é crítico?

A coleta e análise de log é crítica para a capacidade de uma empresa detectar atividades maliciosas rapidamente. Às vezes, os registros de auditoria são a única evidência de um ataque bem-sucedido. Os atacantes sabem que muitas empresas mantêm logs de auditoria para fins de conformidade, mas raramente os analisam. Os atacantes usam esse conhecimento para ocultar sua localização, um software malicioso e as atividades nas máquinas das vítimas. Devido a processos de análise de log insatisfatórios ou inexistentes, os atacantes às vezes controlam as máquinas das vítimas por meses ou anos sem que ninguém na empresa-alvo saiba.

Existem dois tipos de registros que geralmente são tratados e frequentemente configurados de forma independente: logs do sistema e logs de auditoria. Os logs do sistema geralmente fornecem eventos no nível do sistema que mostram vários horários de início/término de processo do sistema, travamentos, etc. Eles são nativos dos sistemas e exigem menos configurações para serem ativados. Os logs de auditoria normalmente incluem eventos no nível do usuário—quando um usuário faz login, acessa um arquivo, etc.—e exige mais planejamento e esforço para configuração.

Os registros de log também são essenciais para a resposta a incidentes. Após a detecção de um ataque, a análise de log pode ajudar as empresas a compreender a extensão de um ataque. Os registros de log completos podem mostrar, por exemplo, quando e como o ataque ocorreu, quais informações foram acessadas e se os dados foram extraídos. A retenção de logs também é crítica no caso de acompanhamento de uma investigação ser necessária ou se um ataque permanecer não detectado por um longo período de tempo.

Procedimentos e ferramentas

A maioria dos ativos e software corporativos oferecem recursos de log. Tal log deve ser ativado, com os logs enviados para servidores de log centralizados. Firewalls, proxies e sistemas de acesso remoto (VPN (Virtual Private Network), dial-up, etc.) devem ser todos configurados para log detalhado quando for benéfico. A retenção de dados de log também é importante no caso de uma investigação de incidente ser necessária.

Além disso, todos os ativos corporativos devem ser configurados para criar logs de controle de acesso quando um usuário tenta acessar recursos sem os privilégios apropriados. Para avaliar se tal log está em vigor, uma empresa deve verificar periodicamente seus logs e compará-los com o inventário de ativos corporativos montado como parte do Controle CIS 1, a fim de garantir que cada ativo gerenciado ativamente conectado à rede está gerando logs periodicamente.

Medidas de Segurança

MEDIDAS DE SEGURANÇA	TÍTULO DA MEDIDA DE SEGURANÇA/ DESCRIÇÃO DA MEDIDA DE SEGURANÇA	TIPO DE ATIVO	FUNÇÃO DE SEGURANÇA	IG1	IG2	IG3
8.1	**Estabelecer e manter um processo de gestão de log de auditoria** Estabeleça e mantenha um processo de gestão de log de auditoria que defina os requisitos de log da empresa. No mínimo, trate da coleta, revisão e retenção de logs de auditoria para ativos corporativos. Revise e atualize a documentação anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.	Rede	Proteger	●	●	●
8.2	**Coletar logs de auditoria** Colete logs de auditoria. Certifique-se de que o log, de acordo com o processo de gestão de log de auditoria da empresa, tenha sido habilitado em todos os ativos.	Rede	Detectar	●	●	●
8.3	**Garantir o armazenamento adequado do registro de auditoria** Certifique-se de que os destinos dos logs mantenham armazenamento adequado para cumprir o processo de gestão de log de auditoria da empresa.	Rede	Proteger	●	●	●
8.4	**Padronizar a sincronização de tempo** Padronize a sincronização de tempo. Configure pelo menos duas fontes de tempo sincronizadas nos ativos corporativos, onde houver suporte.	Rede	Proteger		●	●
8.5	**Coletar logs de auditoria detalhados** Configure o log de auditoria detalhado para ativos corporativos contendo dados sensíveis. Inclua a origem do evento, data, nome de usuário, carimbo de data/hora, endereços de origem, endereços de destino e outros elementos úteis que podem ajudar em uma investigação forense.	Rede	Detectar		●	●
8.6	**Coletar logs de auditoria de consulta dns** Colete logs de auditoria de consulta DNS em ativos corporativos, quando apropriado e suportado.	Rede	Detectar		●	●
8.7	**Coletar logs de auditoria de requisição de url** Colete logs de auditoria de requisição de URL em ativos corporativos, quando apropriado e suportado.	Rede	Detectar		●	●
8.8	**Coletar logs de auditoria de linha de comando** Colete logs de auditoria de linha de comando. Exemplos de implementações incluem a coleta de logs de auditoria do PowerShell®, BASH ™ e terminais administrativos remotos.	Dispositivo	Detectar		●	●
8.9	**Centralizar os logs de auditoria** Centralize, na medida do possível, a coleta e retenção de logs de auditoria nos ativos corporativos.	Rede	Detectar		●	●
8.10	**Reter os logs de auditoria** Reter os logs de auditoria em ativos corporativos por no mínimo 90 dias.	Rede	Proteger		●	●
8.11	**Conduzir revisões de log de auditoria** Realize análises de logs de auditoria para detectar anomalias ou eventos anormais que possam indicar uma ameaça potencial. Realize revisões semanalmente ou com mais frequência.	Rede	Detectar		●	●
8.12	**Colete logs do provedor de serviços** Colete logs do provedor de serviços, onde houver suporte. Exemplos de implementações incluem coleta de eventos de autenticação e autorização, eventos de criação e de descarte de dados e eventos de gestão de usuários.	Dados	Detectar			●

CONTROLE 09

Proteções de e-mail e navegador Web

SAFEGUARDS TOTAL	7	IG1	2/7	IG2	6/7	IG3	7/7

Visão geral

Melhore as proteções e detecções de vetores de ameaças de e-mail e web, pois são oportunidades para atacantes manipularem o comportamento humano por meio do engajamento direto.

Por que este controle é crítico?

Navegadores Web e clientes de e-mail são pontos de entrada muito comuns para atacantes por causa de sua interação direta com usuários dentro de uma empresa. O conteúdo pode ser criado para atrair ou enganar os usuários para que revelem credenciais, forneçam dados sensíveis ou forneçam um canal aberto para permitir que atacantes obtenham acesso, aumentando assim o risco para a empresa. Como o e-mail e a web são os principais meios pelos quais os usuários interagem com usuários e ambientes externos e não confiáveis, esses são os principais alvos tanto de código malicioso quanto de engenharia social. Além disso, conforme as empresas migram para o e-mail baseado na web ou acesso móvel ao e-mail, os usuários não utilizam mais os clientes de e-mail tradicionais com todos os recursos, que fornecem controles de segurança integrados, como criptografia de conexão, autenticação forte e botões de relato de phishing.

Procedimentos e ferramentas

Navegador Web

Os cibercriminosos podem explorar navegadores web de várias maneiras. Se eles tiverem acesso a explorações de navegadores vulneráveis, podem criar páginas web mal-intencionadas que podem explorar essas vulnerabilidades quando navegadas por meio de um navegador inseguro ou sem patch. Como alternativa, podem tentar atingir qualquer número de plug-ins de terceiros de navegadores Web comuns que possam permitir que eles se conectem ao navegador ou mesmo diretamente ao sistema operacional ou aplicação. Esses plug-ins, assim como qualquer outro software em um ambiente, precisam ser revisados quanto a vulnerabilidades, mantidos atualizados com os patches ou versões mais recentes e controlados. Muitos vêm de fontes não confiáveis e alguns até são escritos para serem maliciosos. Portanto, é melhor evitar que os usuários intencionalmente ou não, instalem um malware que possa estar oculto em alguns desses plug-ins, extensões e complementos.

Os navegadores mais populares empregam um banco de dados de sites de phishing e/ou malware para proteger contra as ameaças mais comuns. Uma prática recomendada é habilitar esses filtros de conteúdo e ativar os bloqueadores de pop-up. Os pop-ups não são apenas irritantes; eles também podem hospedar malware embutido diretamente ou induzir os usuários a clicar em links usando truques de engenharia social. Para ajudar a impor o bloqueio de domínios mal-intencionados conhecidos, também considere assinar serviços de filtragem de DNS para bloquear tentativas de acesso a esses sites no nível da rede.

E-mail

O e-mail representa uma das maneiras mais interativas de os humanos trabalharem com ativos corporativos; treinar e encorajar o comportamento correto é tão importante quanto as configurações técnicas. E-mail é o vetor de ameaça mais comum contra empresas por meio de táticas como phishing e Business E-mail Compromise (BEC).

O uso de uma ferramenta de filtragem de spam e verificação de malware no gateway de e-mail reduz o número de e-mails e anexos maliciosos que chegam à rede corporativa. Iniciar o Domain-based Message Authentication, Reporting, and Conformance (DMARC) ajuda a reduzir as atividades de spam e phishing. A instalação de uma ferramenta de criptografia para proteger e-mail e comunicações adiciona outra camada de segurança do usuário e da rede. Além de bloquear com base no remetente, também vale a pena permitir apenas determinados tipos de arquivo que os usuários precisam para seus trabalhos. Isso exigirá coordenação com diferentes unidades de negócios para entender quais tipos de arquivos eles recebem por e-mail para garantir que não haja uma interrupção em seus processos.

Como as técnicas de e-mail phishing estão sempre evoluindo para superar as regras de filtro de SPAM, é importante treinar os usuários sobre como identificar phishing e notificar a segurança de TI quando o virem. Existem muitas plataformas que realizam testes de phishing contra usuários para ajudar a educá-los com diferentes exemplos e monitorar suas melhorias ao longo do tempo. Agrupar esse conhecimento para notificar as equipes de segurança de TI sobre phishing ajuda a melhorar as proteções e detecções de ameaças baseadas em e-mail.

Medidas de Segurança

MEDIDAS DE SEGURANÇA	TÍTULO DA MEDIDA DE SEGURANÇA/ DESCRIÇÃO DA MEDIDA DE SEGURANÇA	TIPO DE ATIVO	FUNÇÃO DE SEGURANÇA	IG1	IG2	IG3
9.1	**Garantir o uso apenas de navegadores e clientes de e-mail suportados plenamente**	Aplicações	Proteger	●	●	●
	Certifique-se de que apenas navegadores e clientes de e-mail suportados plenamente tenham permissão para executar na empresa, usando apenas a versão mais recente dos navegadores e clientes de e-mail fornecidos pelo fornecedor.					
9.2	**Usar serviços de filtragem de DNS**	Rede	Proteger	●	●	●
	Use os serviços de filtragem de DNS em todos os ativos corporativos para bloquear o acesso a domínios mal-intencionados conhecidos.					
9.3	**Manter e impor filtros de URL baseados em rede**	Rede	Proteger		●	●
	Imponha e atualize filtros de URL baseados em rede para limitar um ativo corporativo de se conectar a sites potencialmente maliciosos ou não aprovados. Exemplos de implementações incluem filtragem baseada em categoria, filtragem baseada em reputação ou através do uso de listas de bloqueio. Aplique filtros para todos os ativos corporativos.					

MEDIDAS DE SEGURANÇA	TÍTULO DA MEDIDA DE SEGURANÇA/ DESCRIÇÃO DA MEDIDA DE SEGURANÇA	TIPO DE ATIVO	FUNÇÃO DE SEGURANÇA	IG1	IG2	IG3
9.4	**Restringir extensões de cliente de e-mail e navegador desnecessárias ou não autorizadas** Restrinja, seja desinstalando ou desabilitando, quaisquer plug-ins de cliente de e-mail ou navegador, extensões e aplicações complementares não autorizados ou desnecessários.	Aplicações	Proteger		●	●
9.5	**Implementar o DMARC** Para diminuir a chance de e-mails forjados ou modificados de domínios válidos, implemente a política e verificação DMARC, começando com a implementação dos padrões Sender Policy Framework (SPF) e DomainKeys Identified Mail (DKIM).	Rede	Proteger		●	●
9.6	**Bloquear tipos de arquivo desnecessários** Bloqueie tipos de arquivo desnecessários que tentem entrar no gateway de e-mail da empresa.	Rede	Proteger		●	●
9.7	**Implantar e manter proteções antimalware de servidor de e-mail** Implante e mantenha proteção antimalware de servidores de e-mail, como varredura de anexos e/ou sandbox.	Rede	Proteger			●

CONTROLE 10

Defesas contra malware

SAFEGUARDS TOTAL	7	IG1	3/7	IG2	7/7	IG3	7/7

Visão geral

Impedir ou controlar a instalação, disseminação e execução de aplicações, códigos ou scripts maliciosos em ativos corporativos.

Por que este controle é crítico?

O software malicioso (às vezes classificado como vírus ou Trojans) é um aspecto integrante e perigoso das ameaças da Internet. Eles podem ter várias finalidades, desde capturar credenciais, roubar dados, identificar outros alvos na rede e criptografar ou destruir dados. O malware está em constante evolução e adaptação, à medida que variantes modernas aproveitam as técnicas de aprendizado de máquina.

O malware entra em uma empresa por meio de vulnerabilidades em dispositivos de usuário final, anexos de e-mail, páginas da web, serviços em nuvem, dispositivos móveis e mídia removível. O malware geralmente depende do comportamento inseguro do usuário final, como clicar em links, abrir anexos, instalar software ou perfis, ou inserir unidades flash USB (Universal Serial Bus).

O malware moderno é projetado para evitar, enganar ou desabilitar as defesas. As defesas contra malware devem ser capazes de operar neste ambiente dinâmico por meio de automação, atualização rápida e oportuna e integração com outros processos, como gestão de vulnerabilidade e resposta a incidentes. Eles devem ser implantados em todos os possíveis pontos de entrada e ativos corporativos para detectar, impedir a propagação ou controlar a execução de software ou código malicioso.

Procedimentos e ferramentas

A proteção eficaz contra malware inclui conjuntos tradicionais de prevenção e detecção de malware de endpoint. Para garantir que os IOCs de malware estejam atualizados, as empresas podem receber atualizações automatizadas do fornecedor para enriquecer outros dados de vulnerabilidade ou ameaça. Essas ferramentas são mais bem gerenciadas de forma centralizada para fornecer consistência em toda a infraestrutura.

Ser capaz de bloquear ou identificar malware é apenas parte deste controle CIS; há também foco na coleta centralizada dos logs para oferecer suporte a alertas, identificação e resposta a incidentes. Conforme os atores mal-intencionados continuam a desenvolver suas metodologias, muitos estão começando a adotar uma abordagem de "living-off-the-land" (LotL) para minimizar a probabilidade de serem pegos. Essa abordagem se refere ao comportamento do atacante que usa ferramentas ou recursos que já existem no ambiente de destino. Habilitar o log, de acordo com as medidas de segurança no Controle CIS 8, tornará significativamente mais fácil para a empresa acompanhar os eventos para entender o que aconteceu e por que aconteceu.

Medidas de Segurança

MEDIDAS DE SEGURANÇA	TÍTULO DA MEDIDA DE SEGURANÇA/ DESCRIÇÃO DA MEDIDA DE SEGURANÇA	TIPO DE ATIVO	FUNÇÃO DE SEGURANÇA	IG1	IG2	IG3
10.1	**Instalar e manter um software anti-malware**	**Dispositivo**	**Proteger**	●	●	●
	Instale e mantenha um software anti-malware em todos os ativos corporativos.					
10.2	**Configurar atualizações automáticas de assinatura anti-malware**	**Dispositivo**	**Proteger**	●	●	●
	Configure atualizações automáticas para arquivos de assinatura anti-malware em todos os ativos corporativos.					
10.3	**Desabilitar a execução e reprodução automática para mídias removíveis**	**Dispositivo**	**Proteger**	●	●	●
	Desabilitar a funcionalidade de execução e reprodução automática para mídias removíveis.					
10.4	**Configurar a varredura anti-malware automática de mídia removivel**	**Dispositivo**	**Detectar**		●	●
	Configure o software anti-malware para verificar automaticamente a mídia removível.					
10.5	**Habilitar recursos anti-exploração**	**Dispositivo**	**Proteger**		●	●
	Habilite recursos anti-exploração em ativos e software corporativos, onde possível, como Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), ou Apple® System Integrity Protection (SIP) e Gatekeeper™.					
10.6	**Gerenciar o software anti-malware de maneira centralizada**	**Dispositivo**	**Proteger**		●	●
	Gerencie o software anti-malware de maneira centralizada.					
10.7	**Usar software anti-malware baseado em comportamento**	**Dispositivo**	**Detectar**		●	●
	Use software anti-malware baseado em comportamento.					

CONTROLE 11

Recuperação de dados

SAFEGUARDS TOTAL	5	IG1	4/5	IG2	5/5	IG3	5/5

Visão geral

Estabeleça e mantenha práticas de recuperação de dados suficientes para restaurar ativos corporativos dentro do escopo para um estado pré-incidente e confiável.

Por que este controle é crítico?

Na tríade de segurança cibernética—Confidencialidade, Integridade e Disponibilidade (CID)—a disponibilidade de dados é, em alguns casos, mais crítica do que sua confidencialidade. As empresas precisam de muitos tipos de dados para tomar decisões de negócios e, quando esses dados não estão disponíveis ou não são confiáveis, eles podem impactar a empresa. Um exemplo fácil são as informações meteorológicas para uma empresa de transporte.

Quando os atacantes comprometem os ativos, eles fazem alterações nas configurações, adicionam contas e, frequentemente, adicionam software ou scripts. Essas alterações nem sempre são fáceis de identificar, pois os atacantes podem ter corrompido ou substituído aplicações confiáveis por versões maliciosas ou as alterações podem parecer nomes de conta de aparência padrão. As alterações de configuração podem incluir, adicionar ou alterar entradas de registro, abrir portas, desligar serviços de segurança, excluir logs ou outras ações maliciosas que tornam um sistema inseguro. Essas ações não precisam ser maliciosas; erros humanos também podem causar da mesma forma cada uma delas. Portanto, é importante ter a capacidade de ter backups ou espelhos recentes para recuperar ativos e dados corporativos de volta a um estado confiável conhecido.

Houve um aumento exponencial de ransomware nos últimos anos. Não é uma ameaça nova, embora tenha se tornado mais comercializada e organizada como um método confiável para os atacantes ganharem dinheiro. Se um atacante criptografar os dados de uma empresa e exigir resgate para sua restauração, pode ser útil ter um backup recente para recuperá-los para um estado conhecido e confiável. No entanto, conforme o ransomware evoluiu, ele também se tornou uma técnica de extorsão, em que os dados são extraídos antes de serem criptografados e o atacante pede pagamento para restaurar os dados da empresa, bem como para evitar que sejam vendidos ou divulgados. Nesse caso, a restauração resolveria apenas o problema de restaurar os sistemas a um estado confiável e continuar as operações. Aproveitar a orientação dos Controles CIS ajudará a reduzir o risco de ransomware por meio de uma higiene cibernética aprimorada, já que os atacantes geralmente usam exploits mais antigos ou básicos em sistemas inseguros.

Procedimentos e ferramentas

Os procedimentos de recuperação de dados devem ser definidos no processo de gestão de dados descrito em Controle CIS 3, Proteção de Dados. Isso deve incluir procedimentos de backup com base no valor dos dados, sensibilidade ou requisitos de retenção. Isso ajudará a desenvolver a frequência e o tipo de backup (completo vs. incremental).

Uma vez por trimestre (ou sempre que um novo processo ou tecnologia de backup for introduzido), uma equipe de teste deve avaliar uma amostra aleatória de backups e tentar restaurá-los em um ambiente de teste. Os backups restaurados devem ser verificados para garantir que o sistema operacional, a aplicação e dados do backup estejam intactos e funcionais.

No caso de infecção por malware, os procedimentos de restauração devem usar uma versão do backup que se acredita ser anterior à infecção original.

Medidas de Segurança

MEDIDAS DE SEGURANÇA	TÍTULO DA MEDIDA DE SEGURANÇA/ DESCRIÇÃO DA MEDIDA DE SEGURANÇA	TIPO DE ATIVO	FUNÇÃO DE SEGURANÇA	IG1	IG2	IG3
11.1	**Estabelecer e manter um processo de recuperação de dados** Estabeleça e mantenha um processo de recuperação de dados. No processo, aborde o escopo das atividades de recuperação de dados, a priorização da recuperação e a segurança dos dados de backup. Revise e atualize a documentação anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.	Dados	Recuperar	●	●	●
11.2	**Executar backups automatizados** Execute backups automatizados de ativos corporativos dentro do escopo. Execute backups semanalmente ou com mais frequência, com base na sensibilidade dos dados.	Dados	Recuperar	●	●	●
11.3	**Proteger os dados de recuperação** Proteja os dados de recuperação com controles equivalentes dos dados originais. Referencie o uso de criptografia ou separação de dados, com base nos requisitos.	Dados	Proteger	●	●	●
11.4	**Estabelecer e manter uma instância isolada de dados de recuperação** Estabeleça e mantenha uma instância isolada de dados de recuperação. Exemplos de implementações incluem controle de versão de destinos de backup por meio de sistemas ou serviços offline, na nuvem ou fora do site local.	Dados	Recuperar	●	●	●
11.5	**Testar os dados de recuperação** Teste a recuperação do backup trimestralmente, ou com mais frequência, para uma amostra dos ativos corporativos dentro do escopo.	Dados	Recuperar		●	●

CONTROLE 12

Gestão da infraestrutura de rede

SAFEGUARDS TOTAL	8	IG1	1/8	IG2	7/8	IG3	8/8

Visão geral

Estabeleça, implemente e gerencie ativamente (rastreie, reporte, corrija) os dispositivos de rede, a fim de evitar que atacantes explorem serviços de rede e pontos de acesso vulneráveis.

Por que este controle é crítico?

A infraestrutura de rede segura é uma defesa essencial contra ataques. Isso inclui uma arquitetura de segurança apropriada, abordando vulnerabilidades que são, muitas vezes, introduzidas com configurações padrão, monitoramento de alterações e reavaliação das configurações atuais. A infraestrutura de rede inclui dispositivos como gateways físicos e virtualizados, firewalls, pontos de acesso sem fio, roteadores e switches.

As configurações padrão para dispositivos de rede são voltadas para facilidade de implantação e uso—não para segurança. Potenciais vulnerabilidades padrão incluem portas e serviços abertos, contas e senhas padrão (incluindo contas de serviço), suporte para protocolos vulneráveis mais antigos e pré-instalação de software desnecessário. Os atacantes procuram configurações padrão vulneráveis, lacunas ou inconsistências em conjuntos de regras de firewall, roteadores e switches e usam essas lacunas para penetrar nas defesas. Eles exploram falhas nesses dispositivos para obter acesso às redes, redirecionar o tráfego em uma rede e interceptar dados durante a transmissão.

A segurança da rede é um ambiente em constante mudança que exige uma reavaliação regular dos diagramas de arquitetura, configurações, controles de acesso e fluxos de tráfego permitidos. Os atacantes tiram proveito das configurações de dispositivos de rede que se tornam menos seguras com o tempo, à medida que os usuários exigem exceções para necessidades de negócio específicas. Às vezes, as exceções são implantadas, mas não removidas quando não são mais aplicáveis às necessidades do negócio. Em alguns casos, o risco de segurança de uma exceção não é devidamente analisado nem medido em relação à necessidade de negócios associada e pode mudar com o tempo.

Procedimentos e ferramentas

As empresas devem garantir que a infraestrutura de rede seja totalmente documentada e os diagramas de arquitetura sejam mantidos atualizados. É importante que os principais componentes da infraestrutura tenham o suporte do fornecedor para patches e atualizações de funcionalidades. Atualize os componentes em fim de ciclo de vida (EOL) antes da data em que eles ficarão sem suporte ou aplique controles de mitigação para isolá-los. As empresas precisam monitorar suas versões e configurações de infraestrutura em busca de vulnerabilidades que exigem que se atualize os dispositivos de rede para a versão segura e estável mais recente que não impacte a infraestrutura.

Um diagrama de arquitetura de rede atualizado, incluindo diagramas de arquitetura de segurança, é uma base importante para a gestão de infraestrutura. O próximo passo é ter uma gestão completa de contas para controle de acesso, log e monitoramento. Finalmente, a administração da infraestrutura só deve ser realizada em protocolos seguros, com autenticação forte (MFA para PAM) e a partir de dispositivos administrativos dedicados ou redes fora de banda.

Ferramentas de mercado podem ser úteis para avaliar os conjuntos de regras de dispositivos de filtragem de rede para determinar se eles estão consistentes ou em conflito. Isso fornece uma verificação de integridade automatizada dos filtros de rede. Essas ferramentas procuram erros em conjuntos de regras ou Access Controls Lists (ACLs) que podem permitir serviços indesejados por meio do dispositivo de rede. Essas ferramentas devem ser executadas sempre que mudanças significativas forem feitas nos conjuntos de regras do firewall, ACLs do roteador ou outras tecnologias de filtragem.

→ **Para orientação sobre teletrabalho e pequenos escritórios, consulte o CIS Controls Telework and Small Office Network Security Guide:** https://www.cisecurity.org/controls/v8/

Medidas de Segurança

MEDIDAS DE SEGURANÇA	TÍTULO DA MEDIDA DE SEGURANÇA/ DESCRIÇÃO DA MEDIDA DE SEGURANÇA	TIPO DE ATIVO	FUNÇÃO DE SEGURANÇA	IG1	IG2	IG3
12.1	**Assegurar que a infraestrutura de rede esteja atualizada** Assegure que a infraestrutura de rede seja mantida atualizada. Exemplos de implementações incluem a execução da versão estável mais recente do software e/ou o uso de ofertas de network-as-a-service (NaaS) atualmente suportadas. Revise as versões do software mensalmente, ou com mais frequência, para verificar o suporte do software.	Rede	Proteger	●	●	●
12.2	**Estabelecer e manter uma arquitetura de rede segura** Estabeleça e mantenha uma arquitetura de rede segura. Uma arquitetura de rede segura deve abordar segmentação, privilégio mínimo e disponibilidade, no mínimo.	Rede	Proteger		●	●
12.3	**Gerenciar infraestrutura de rede com segurança** Gerencie com segurança a infraestrutura de rede. Exemplos de implementações incluem versão controlada de infraestrutura como código e o uso de protocolos de rede seguros, como SSH e HTTPS.	Rede	Proteger		●	●
12.4	**Estabelecer e manter diagrama(s) de arquitetura** Estabeleça e mantenha diagrama(s) de arquitetura e/ou outra documentação de sistema de rede. Revise e atualize a documentação anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.	Rede	Identificar		●	●

MEDIDAS DE SEGURANÇA	TÍTULO DA MEDIDA DE SEGURANÇA/ DESCRIÇÃO DA MEDIDA DE SEGURANÇA	TIPO DE ATIVO	FUNÇÃO DE SEGURANÇA	IG1	IG2	IG3
12.5	**Centralizar a autenticação, autorização e auditoria (AAA) de rede** Centralize AAA de rede.	Rede	Proteger		●	●
12.6	**Usar protocolos de comunicação e gestão de rede seguros** Use protocolos de comunicação e gestão de rede seguros (por exemplo, 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise ou superior).	Rede	Proteger		●	●
12.7	**Assegurar que os dispositivos remotos utilizem uma VPN e estejam se conectando a uma infraestrutura AAA da empresa** Exigir que os usuários se autentiquem em serviços de autenticação e VPN gerenciados pela empresa antes de acessar os recursos da empresa em dispositivos de usuário final.	Dispositivo	Proteger		●	●
12.8	**Estabelecer e manter recursos de computação dedicados para todo o trabalho administrativo** Estabeleça e mantenha recursos de computação dedicados, fisicamente ou logicamente separados, para todas as tarefas administrativas ou tarefas que requeiram acesso administrativo. Os recursos de computação devem ser segmentados da rede primária da empresa e não deve ser permitido o acesso à Internet.	Dispositivo	Proteger			●

CONTROLE 13

Monitoramento e defesa da Rede

SAFEGUARDS TOTAL 11 | IG1 0/11 | IG2 6/11 | IG3 11/11

Visão geral

Operar processos e ferramentas para estabelecer e manter monitoramento e defesa de rede abrangente contra ameaças de segurança em toda a infraestrutura de rede corporativa e base de usuários.

Por que este controle é crítico?

Não podemos confiar que as defesas da rede sejam perfeitas. Os adversários continuam a evoluir e amadurecer, à medida que compartilham ou vendem informações entre sua comunidade sobre exploits e desvios para controles de segurança. Mesmo que as ferramentas de segurança funcionem "conforme anunciado", é necessário um entendimento da postura de risco corporativo para configurá-las, ajustá-las e registrá-las em log para serem eficazes. Frequentemente, configurações incorretas devido a erro humano ou falta de conhecimento dos recursos da ferramenta dão às empresas uma falsa sensação de segurança.

As ferramentas de segurança só podem ser eficazes se oferecerem suporte a um processo de monitoramento contínuo que permita à equipe ser alertada e responder rapidamente a incidentes de segurança. As empresas que adotam uma abordagem puramente orientada para a tecnologia também terão mais falsos positivos, devido ao excesso de confiança nos alertas das ferramentas. Identificar e responder a essas ameaças requer visibilidade de todos os vetores de ameaças da infraestrutura e aproveitamento de pessoas no processo de detecção, análise e resposta. É essencial para empresas grandes ou fortemente direcionadas ter uma capacidade de operações de segurança para prevenir, detectar e responder rapidamente às ameaças cibernéticas antes que elas possam impactar a empresa. Este processo irá gerar relatórios de atividades e métricas que ajudarão a aprimorar as políticas de segurança e apoiar a conformidade regulatória para muitas empresas.

Como temos visto muitas vezes na imprensa, as empresas têm sido comprometidas por semanas, meses ou anos antes de serem descobertas. O principal benefício de ter uma consciência situacional abrangente é aumentar a velocidade de detecção e resposta. Isso é fundamental para responder rapidamente quando um malware é descoberto, credenciais são roubadas ou quando dados sensíveis são comprometidos para reduzir o impacto para a empresa.

Por meio de uma boa conscientização situacional (ou seja, operações de segurança), as empresas irão identificar e catalogar Táticas, Técnicas e Procedimentos (TTPs) de atacantes, incluindo seus IOCs que ajudarão a empresa a se tornar mais proativa na identificação de futuras ameaças ou incidentes. A recuperação pode ser alcançada mais rapidamente quando a resposta tem acesso a informações completas sobre o ambiente e a estrutura da empresa para desenvolver estratégias de resposta eficientes.

Procedimentos e ferramentas

A maioria das empresas não precisa de um Security Operations Center (SOC) para obter consciência situacional. Isso começa com a compreensão das funções críticas de negócios, arquiteturas de rede e servidor, dados e fluxos de dados, serviços de fornecedores e conexão de parceiro de negócios, e dispositivos e contas de usuário final. Isso informa o desenvolvimento de uma arquitetura de segurança, controles técnicos, log, monitoramento e procedimentos de resposta.

No centro desse processo está uma equipe treinada e organizada que implementa processos para detecção, análise e mitigação de incidentes. Esses recursos podem ser conduzidos internamente, ou por meio de consultores ou um provedor de serviços gerenciados. As empresas devem considerar atividades de rede, ativos corporativos, credenciais do usuário e acesso a dados. A tecnologia desempenhará um papel crucial para coletar e analisar todos os dados e monitorar redes e ativos corporativos interna e externamente à empresa. As empresas devem incluir visibilidade para plataformas em nuvem que podem não estar de acordo com a tecnologia de segurança local.

O encaminhamento de todos os registros importantes para programas de análise, como soluções de gestão de informações e eventos de segurança (SIEM), pode agregar valor; no entanto, eles não fornecem uma fotografia completa. Revisões semanais de log são necessárias para ajustar os limites e identificar eventos anormais. As ferramentas de correlação podem tornar os logs de auditoria mais úteis para a inspeção manual subsequente. Essas ferramentas não substituem pessoal qualificado em segurança da informação e administradores de sistema. Mesmo com ferramentas automatizadas de análise de log, experiência humana e intuição são frequentemente necessárias para identificar e compreender os ataques.

À medida que esse processo amadurece, as empresas criarão, manterão e desenvolverão uma base de conhecimento que ajudará a compreender e avaliar os riscos do negócio, desenvolvendo uma capacidade interna de inteligência de ameaças. Inteligência de ameaças é a coleção de TTPs de incidentes e adversários. Para conseguir isso, um programa de conscientização situacional definirá e avaliará quais fontes de informação são relevantes para detectar, relatar e lidar com ataques. A maioria das empresas maduras pode evoluir para a caça a ameaças, em que uma equipe treinada analisa manualmente os registros do sistema e do usuário, fluxos de dados e padrões de tráfego para encontrar anomalias.

Medidas de Segurança

MEDIDAS DE SEGURANÇA	TÍTULO DA MEDIDA DE SEGURANÇA/ DESCRIÇÃO DA MEDIDA DE SEGURANÇA	TIPO DE ATIVO	FUNÇÃO DE SEGURANÇA	IG1	IG2	IG3
13.1	**Centralizar o alerta de eventos de segurança** Centralize os alertas de eventos de segurança em ativos corporativos para correlação e análise de log. A melhor prática requer o uso de um SIEM, que inclui alertas de correlação de eventos definidos pelo fornecedor. Uma plataforma de análise de log configurada com alertas de correlação relevantes para a segurança também atende a esta medida de segurança.	Rede	Detectar		●	●
13.2	**Implantar solução de detecção de intrusão baseada em host** Implante uma solução de detecção de intrusão baseada em host em ativos corporativos, quando apropriado e/ou com suporte.	Dispositivo	Detectar		●	●
13.3	**Implantar uma solução de detecção de intrusão de rede** Implante uma solução de detecção de intrusão de rede em ativos corporativos, quando apropriado. Exemplos de implementações incluem o uso de um Network Intrusion Detection System (NIDS) ou serviço de provedor de serviço de nuvem equivalente (CSP).	Rede	Detectar		●	●
13.4	**Realizar filtragem de tráfego entre segmentos de rede** Execute a filtragem de tráfego entre segmentos de rede, quando apropriado.	Rede	Proteger		●	●
13.5	**Gerenciar controle de acesso para ativos remotos** Gerencie o controle de acesso para ativos que se conectam remotamente aos recursos da empresa. Determine a quantidade de acesso aos recursos da empresa com base em: software anti-malware atualizado instalado, conformidade de configuração com o processo de configurações seguras da empresa e garantia de que o sistema operacional e as aplicações estão atualizados.	Dispositivo	Proteger		●	●
13.6	**Coletar logs de fluxo de tráfego da rede** Colete logs de fluxo de tráfego de rede e/ou tráfego de rede para revisar e alertar sobre dispositivos de rede.	Rede	Detectar		●	●
13.7	**Implantar solução de prevenção de intrusão baseada em host** Implante uma solução de prevenção de intrusão baseada em host em ativos corporativos, quando apropriado e/ou com suporte. Exemplos de implementações incluem o uso de um cliente Endpoint Detection and Response (EDR) ou agente IPS baseado em host.	Dispositivo	Proteger			●
13.8	**Implantar uma solução de prevenção de intrusão de rede** Implante uma solução de prevenção de intrusão de rede, quando apropriado. Exemplos de implementações incluem o uso de um Network Intrusion Prevention System (NIPS) ou serviço CSP equivalente.	Rede	Proteger			●
13.9	**Implantar controle de acesso no nível de porta** Implante o controle de acesso no nível de porta. O controle de acesso no nível de porta utiliza 802.1x ou protocolos de controle de acesso à rede semelhantes, como certificados, e pode incorporar autenticação de usuário e/ou dispositivo.	Dispositivo	Proteger			●
13.10	**Executar filtragem da camada de aplicação** Execute a filtragem da camada de aplicação. Exemplos de implementações incluem um proxy de filtragem, firewall de camada de aplicação ou gateway.	Rede	Proteger			●
13.11	**Ajustar Limites de Alerta de Eventos de Segurança** Ajuste os limites de alerta de eventos de segurança mensalmente ou com mais frequência.	Rede	Detectar			●

CONTROLE 14

Conscientização sobre segurança e treinamento de competências

SAFEGUARDS TOTAL	9	IG1	8/9	IG2	9/9	IG3	9/9

Visão geral

Estabelecer e manter um programa de conscientização de segurança para influenciar o comportamento da força de trabalho para ser consciente em segurança e devidamente qualificada para reduzir os riscos de segurança cibernética para a empresa.

Por que este controle é crítico?

As ações das pessoas desempenham um papel crítico no sucesso ou no fracasso do programa de segurança de uma empresa. É mais fácil para um atacante induzir um usuário a clicar em um link ou abrir um anexo de e-mail para instalar malware para entrar em uma empresa do que encontrar um exploit de rede para fazê-lo diretamente.

Os próprios usuários, intencionalmente ou não, podem causar incidentes como resultado do manuseio incorreto de dados sensíveis, enviar um e-mail com dados sensíveis para o destinatário errado, perder um dispositivo de usuário final portátil, usar senhas fracas ou usar a mesma senha que usam em sites públicos.

Nenhum programa de segurança pode lidar com o risco cibernético de maneira eficaz sem um meio de lidar com essa vulnerabilidade humana fundamental. Os usuários em todos os níveis da empresa têm riscos diferentes. Por exemplo: executivos gerenciam dados mais sensíveis; os administradores de sistema têm a capacidade de controlar o acesso a sistemas e aplicações; e usuários em finanças, recursos humanos e contratos, todos têm acesso a diferentes tipos de dados sensíveis que podem torná-los alvos.

O treinamento deve ser atualizado regularmente. Isso aumentará a cultura de segurança e irá desencorajar soluções alternativas arriscadas.

Procedimentos e ferramentas

Um programa de treinamento de conscientização de segurança eficaz não deve ser apenas um vídeo de treinamento enlatado, uma vez por ano, juntamente com testes regulares de phishing. Embora o treinamento anual seja necessário, também deve haver mensagens e notificações mais frequentes sobre a segurança. Isso pode incluir mensagens sobre: uso de senha forte que coincide com um relato da mídia de dump de senha, aumento de phishing durante a época dos impostos ou maior conscientização sobre e-mails de entrega de pacotes maliciosos durante os feriados.

O treinamento também deve levar em consideração as diferentes posturas regulatórias e de ameaças da empresa. As empresas financeiras podem ter mais treinamento relacionado à conformidade sobre manuseio e uso de dados, empresas de saúde sobre como lidar com dados de saúde e comerciantes para dados de cartão de crédito.

O treinamento de engenharia social, como testes de phishing, também deve incluir o conhecimento de táticas que visam diferentes funções. Por exemplo, a equipe financeira receberá tentativas de BEC se passando por executivos pedindo para transferir dinheiro ou receberá e-mails de parceiros comprometidos ou fornecedores solicitando a alteração das informações da conta bancária para o próximo pagamento.

Para um tratamento mais abrangente deste tópico, os seguintes recursos são úteis para construir um programa de conscientização de segurança eficaz:

- **NIST® SP 800-50 Infosec Awareness Training:** https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf
- **National Cyber Security Center (Reino Unido):** https://www.ncsc.gov.uk/guidance/10-steps-user-education-and-awareness
- **EDUCAUSE:** https://www.educause.edu/focus-areas-and-initiatives/policyandsecurity/cybersecurity-program/awareness-campaigns
- **National Cyber Security Alliance (NCSA:** https://staysafeonline.org/
- **SANS:** https://www.sans.org/security-awareness-training/resources
- **Para obter orientação sobre como configurar roteadores domésticos, consulte o CIS Controls Telework and Small Office Network Security Guide:** https://www.cisecurity.org/white-papers/cis-controls-telework-and-small-office-network-security-guide/

Medidas de Segurança

MEDIDAS DE SEGURANÇA	TÍTULO DA MEDIDA DE SEGURANÇA/ DESCRIÇÃO DA MEDIDA DE SEGURANÇA	TIPO DE ATIVO	FUNÇÃO DE SEGURANÇA	IG1	IG2	IG3
14.1	**Estabelecer e manter um programa de conscientização de segurança** Estabeleça e mantenha um programa de conscientização de segurança. O objetivo de um programa de conscientização de segurança é educar a força de trabalho da empresa sobre como interagir com ativos e dados corporativos de maneira segura. Realize o treinamento na contratação e, no mínimo, anualmente. Revise e atualize o conteúdo anualmente ou quando ocorrerem mudanças significativas na empresa que possam afetar esta proteção.	N/A	Proteger	●	●	●
14.2	**Treinar membros da força de trabalho para reconhecer ataques de engenharia social** Treine os membros da força de trabalho para reconhecer ataques de engenharia social, como phishing, pretexto e uso não autorizado.	N/A	Proteger	●	●	●
14.3	**Treinar membros da força de trabalho nas melhores práticas de autenticação** Treine os membros da força de trabalho nas melhores práticas de autenticação. Exemplos de tópicos incluem MFA, composição de senha e gestão de credenciais	N/A	Proteger	●	●	●

MEDIDAS DE SEGURANÇA	TÍTULO DA MEDIDA DE SEGURANÇA/ DESCRIÇÃO DA MEDIDA DE SEGURANÇA	TIPO DE ATIVO	FUNÇÃO DE SEGURANÇA	IG1	IG2	IG3
14.4	**Treinar a força de trabalho nas Melhores Práticas de Tratamento de Dados** Treine os membros da força de trabalho sobre como identificar, armazenar, transferir, arquivar e destruir dados sensíveis de maneira adequada. Isso também inclui o treinamento de membros da força de trabalho em práticas recomendadas de mesa e tela limpas, como bloquear a tela quando eles se afastam de seus ativos corporativos, apagar quadros brancos físicos e virtuais no final das reuniões e armazenar dados e ativos com segurança.	N/A	Proteger	●	●	●
14.5	**Treinar membros da força de trabalho sobre as causas da exposição não intencional de dados** Treine os membros da força de trabalho para estarem cientes das causas da exposição não intencional de dados. Exemplos de tópicos incluem entrega incorreta de dados sensíveis, perda de um dispositivo de usuário final portátil ou publicação de dados para públicos indesejados.	N/A	Proteger	●	●	●
14.6	**Treinar Membros da força de trabalho no Reconhecimento e Comunicação de Incidentes de Segurança** Treine os membros da força de trabalho para serem capazes de reconhecer um incidente em potencial e relatar tal incidente.	N/A	Proteger	●	●	●
14.7	**Treinar a força de trabalho sobre como identificar e comunicar se o seus ativos corporativos estão faltando atualizações de segurança** Treine a força de trabalho para entender como verificar e relatar patches de software desatualizados ou quaisquer falhas em ferramentas e processos automatizados. Parte desse treinamento deve incluir a notificação do pessoal de TI sobre quaisquer falhas em processos e ferramentas automatizadas.	N/A	Proteger	●	●	●
14.8	**Treinar a força de trabalho sobre os perigos de se conectar e transmitir dados corporativos em redes inseguras** Treine os membros da força de trabalho sobre os perigos de se conectar e transmitir dados em redes inseguras para atividades corporativas. Se a empresa tiver funcionários remotos, o treinamento deve incluir orientação para garantir que todos os usuários configurem com segurança sua infraestrutura de rede doméstica.	N/A	Proteger	●	●	●
14.9	**Conduzir treinamento de competências e conscientização de segurança para funções específicas** Conduza treinamento de conscientização de segurança e de competências específicas para funções. Exemplos de implementações incluem cursos de administração de sistema seguro para profissionais de TI, treinamento de conscientização e prevenção de vulnerabilidades para desenvolvedores de aplicações da web do OWASP® Top 10 aplicações e treinamento avançado de conscientização de engenharia social para funções de perfil alto.	N/A	Proteger		●	●

CONTROLE 15

Gestão de provedor de serviços

SAFEGUARDS TOTAL	7	IG1	1/7	IG2	4/7	IG3	7/7

Visão geral

Desenvolva um processo para avaliar os provedores de serviços que mantêm dados sensíveis, ou são responsáveis por plataformas ou processos de TI críticos de uma empresa, para garantir que esses provedores estejam protegendo essas plataformas e dados de forma adequada.

Por que este controle é crítico?

Em nosso mundo moderno e conectado, as empresas contam com fornecedores e parceiros para ajudar a gerenciar seus dados ou contam com infraestrutura de terceiros para aplicações ou funções essenciais.

Houve vários exemplos em que violações de terceiros impactaram significativamente uma empresa; por exemplo, no final dos anos 2000, cartões de pagamento foram comprometidos depois que atacantes se infiltraram em pequenos fornecedores terceirizados no setor de varejo.

Os exemplos mais recentes incluem ataques de ransomware que afetam uma empresa indiretamente, devido ao bloqueio de um de seus provedores de serviço, causando interrupção nos negócios. Ou pior, se conectado diretamente, um ataque de ransomware pode criptografar dados na empresa principal.

A maioria das regulamentações de segurança e privacidade de dados exige que sua proteção seja estendida a prestadores de serviços terceirizados, como acordos de parceiros comerciais de Health Insurance Portability and Accountability Act (HIPAA) na área de saúde, requisitos do Federal Financial Institutions Examination Council (FFIEC) para o setor financeiro e o United Kingdom (UK) Cyber Essentials. A confiança de terceiros é uma função central de Governança, Riscos e Compliance (GRC), pois os riscos que não são gerenciados dentro da empresa são transferidos para entidades fora da empresa.

Embora a revisão da segurança de terceiros seja uma tarefa realizada por décadas, não existe um padrão universal para avaliar a segurança; e, muitos provedores de serviço estão sendo auditados por seus clientes várias vezes ao mês, causando impactos em sua própria produtividade. Isso ocorre porque cada empresa tem um "checklist" diferente ou conjunto de padrões para classificar o provedor de serviços. Existem apenas alguns padrões da indústria, como em finanças, com o programa Shared Assessments, ou no ensino superior, com seu Higher Education Community Vendor Assessment Toolkit (HECVAT). As seguradoras que vendem apólices de segurança cibernética também têm suas próprias medidas.

Embora uma empresa possa fazer um exame muito minucioso em grandes empresas de hospedagem de aplicações ou de nuvem porque estão hospedando seus e-mails ou aplicações de negócios essenciais, as empresas menores costumam apresentar risco maior. Frequentemente, um provedor de serviços terceirizado contrata terceiros para fornecer outros plug-ins ou serviços, tais como quando um terceiro usa uma plataforma ou produto de outros terceiros para oferecer suporte à empresa principal.

Procedimentos e ferramentas

A maioria das empresas tradicionalmente usa checklists padrão, como os da ISO 27001 ou os Controles CIS. Frequentemente, esse processo é gerenciado por meio de planilhas; no entanto, existem plataformas online agora que permitem a gestão centralizada desse processo. O foco deste Controle CIS, porém, não está no checklist; em vez disso, está nos fundamentos do programa. Certifique-se de revisitar anualmente, pois as relações e os dados podem mudar.

Não importa o tamanho da empresa, deve haver uma política sobre a revisão dos prestadores de serviços, um inventário desses fornecedores e uma classificação de risco associada ao seu impacto potencial para os negócios em caso de um incidente. Também deve haver linguagem nos contratos para responsabilizá-los se houver um incidente que afete a empresa.

Existem plataformas de avaliação de terceiros que possuem um inventário de milhares de provedores de serviços, que tentam fornecer uma visão central do setor, para ajudar as empresas a tomar decisões de risco mais informadas. Essas plataformas costumam ter uma pontuação de risco dinâmica para prestadores de serviços, com base (geralmente) em avaliações técnicas passivas ou enriquecidas por meio de avaliações de terceiros de outras empresas.

Ao realizar as revisões, concentre-se nos serviços ou departamentos do provedor que dão suporte à empresa. Um terceiro que tenha um contrato de serviço de segurança gerenciado, ou aderente, e tenha seguro de segurança cibernética, também pode ajudar na redução de riscos.

Também é importante descomissionar com segurança os prestadores de serviços quando os contratos são concluídos ou rescindidos. As atividades de descomissionamento podem incluir a desativação das contas de usuário e de serviço, o encerramento dos fluxos de dados e o descarte seguro de dados corporativos nos sistemas do provedor de serviços.

→ **Referir ao NIST® 800-88r1:** Guidelines for Media Sanitization, conforme apropriado: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf.

Medidas de Segurança

MEDIDAS DE SEGURANÇA	TÍTULO DA MEDIDA DE SEGURANÇA/ DESCRIÇÃO DA MEDIDA DE SEGURANÇA	TIPO DE ATIVO	FUNÇÃO DE SEGURANÇA	IG1	IG2	IG3
15.1	**Estabelecer e manter um inventário de provedores de serviços** Estabeleça e mantenha um inventário de provedores de serviço. O inventário deve listar todos os provedores de serviços conhecidos, incluir classificação(ões) e designar um contato corporativo para cada provedor de serviços. Revise e atualize o inventário anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.	N/A	Identificar	●	●	●
15.2	**Estabelecer e manter uma política de gestão de provedores de serviços** Estabeleça e mantenha uma política de gestão de provedores de serviços. Certifique-se de que a política trate da classificação, inventário, avaliação, monitoramento e descomissionamento de prestadores de serviços. Revise e atualize a política anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.	N/A	Identificar		●	●
15.3	**Classificar provedores de serviços** Classifique os provedores de serviço. A consideração de classificação pode incluir uma ou mais características, como sensibilidade de dados, volume de dados, requisitos de disponibilidade, regulamentos aplicáveis, risco inerente e risco mitigado. Atualize e analise as classificações anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.	N/A	Identificar		●	●
15.4	**Garantir que os contratos do provedor de serviços incluam requisitos de segurança** Certifique-se de que os contratos do provedor de serviços incluem requisitos de segurança. Requisitos de exemplo podem incluir requisitos mínimos do programa de segurança, notificação e resposta de incidente de segurança e/ou de violação de dados, requisitos de criptografia de dados e compromissos de descarte de dados. Esses requisitos de segurança devem ser consistentes com a política de gestão do provedor de serviços da empresa. Revise os contratos do provedor de serviços anualmente para garantir que os contratos não estejam perdendo os requisitos de segurança.	N/A	Proteger		●	●
15.5	**Avaliar provedores de serviços** Avalie os provedores de serviços consistentes com a política de gestão de provedores de serviços da empresa. O escopo da avaliação pode variar com base na(s) classificação(ões) e pode incluir a revisão dos relatórios de avaliação padronizados, como Service Organization Control 2 (SOC 2) e Payment Card Industry (PCI) Attestation of Compliance (AoC), questionários personalizados ou outros processos rigorosos apropriados. Reavalie os prestadores de serviços anualmente, no mínimo, ou com contratos novos e renovados.	N/A	Identificar			●
15.6	**Monitorar provedores de serviços** Monitore os provedores de serviços de acordo com a política de gestão de provedores de serviços da empresa. O monitoramento pode incluir reavaliação periódica da conformidade do provedor de serviços, monitoramento dos release notes do provedor de serviços e monitoramento da dark web.	Dados	Detectar			●
15.7	**Descomissionar com segurança os provedores de serviços** Descomissione os prestadores de serviços com segurança. Considerações de exemplo incluem desativação de contas de usuário e serviço, encerramento de fluxos de dados e descarte seguro de dados corporativos em sistemas de provedores de serviços.	Dados	Proteger			●

CONTROLE 16

Segurança de aplicações

SAFEGUARDS TOTAL	14	IG1	0/14	IG2	11/14	IG3	14/14

Visão geral

Gerencie o ciclo de vida da segurança de software desenvolvido, hospedado ou adquirido internamente para prevenir, detectar e corrigir os pontos fracos de segurança antes que possam afetar a empresa.

Por que este controle é crítico?

As aplicações fornecem uma interface amigável para permitir que os usuários acessem e gerenciem dados de uma forma alinhada às funções de negócios. Eles também minimizam a necessidade de os usuários lidarem diretamente com funções de sistema complexas (e potencialmente sujeitas a erros), como fazer login em um banco de dados para inserir ou modificar arquivos. As empresas usam aplicações para gerenciar seus dados mais sensíveis e controlar o acesso aos recursos do sistema. Portanto, um atacante pode usar a própria aplicação para comprometer os dados, em vez de uma sequência elaborada de invasão de rede e sistema que tenta desviar dos controles e sensores de segurança da rede. É por isso que proteger as credenciais do usuário (especificamente as credenciais da aplicação) definidas no Controle CIS 6 é tão importante.

Na ausência de credenciais, as falhas de aplicação são a escolha para os vetores de ataque. No entanto, as aplicações de hoje são desenvolvidas, operadas e mantidas em um ambiente altamente complexo, diverso e dinâmico. As aplicações são executadas em várias plataformas: web, móvel, nuvem, etc., com arquiteturas de aplicações que são mais complexas do que as estruturas legadas de cliente-servidor ou servidor de banco de dados web. Os ciclos de vida de desenvolvimento tornaram-se mais curtos, passando de meses ou anos em longas metodologias em cascata para ciclos de DevOps com atualizações de código frequentes. Além disso, as aplicações raramente são criadas do zero e geralmente são “montadas” a partir de uma combinação complexa de estruturas de desenvolvimento, bibliotecas, código existente e novos códigos. Existem também regulamentações de proteção de dados modernas e em evolução que tratam da privacidade do usuário. Isso pode exigir conformidade com requisitos de proteção de dados específicos do setor ou regionais.

Esses fatores tornam as abordagens tradicionais de segurança, como controle (de processos, fontes de código, ambiente de tempo de execução, etc.), inspeção e teste, muito mais desafiadoras. Além disso, o risco que uma vulnerabilidade de aplicação apresenta pode não ser compreendido, exceto em uma configuração ou contexto operacional específico.

As vulnerabilidades de aplicação podem estar presentes por vários motivos: design inseguro, infraestrutura insegura, erros de codificação, autenticação fraca e falha no teste para condições incomuns ou inesperadas. Os atacantes podem explorar vulnerabilidades específicas, incluindo buffer overflows, exposição à Structured Query Language (SQL) injection, cross-site scripting, falsificação de solicitações entre sites e click-jacking de código para obter acesso a dados sensíveis ou assumir o controle de ativos vulneráveis dentro da infraestrutura como um ponto de partida para novos ataques.

Aplicações e sites também podem ser usados para coletar credenciais, dados ou tentar instalar malware nos usuários que os acessam.

Finalmente, agora é mais comum adquirir plataformas de Software as a Service (SaaS), nas quais o software é desenvolvido e gerenciado inteiramente por terceiros. Eles podem ser hospedados em qualquer lugar do mundo. Isso traz desafios para as empresas que precisam saber quais riscos estão aceitando ao usar essas plataformas; e, muitas vezes, não têm visibilidade das práticas de desenvolvimento e segurança de aplicações dessas plataformas. Algumas dessas plataformas SaaS permitem a personalização de suas interfaces e bancos de dados. As empresas que estendem esses aplicações devem seguir este Controle CIS, semelhante a se estivessem fazendo o desenvolvimento de cliente desde o início.

Procedimentos e ferramentas

Para a versão 8, o CIS fez parceria com a SAFECode para ajudar a desenvolver os procedimentos e proteções para esta atualização do Controle de Segurança de Software de a aplicação. No entanto, a segurança do software de aplicação é um grande tópico por si só e, portanto (de acordo com os princípios dos Controles CIS gerais), nos concentramos aqui nas proteções mais críticas. Elas foram derivadas de um documento complementar sobre segurança de software de aplicação que o SAFECode desenvolveu (referenciado abaixo), que fornece um tratamento mais aprofundado do tópico e é consistente com o corpo de conteúdo existente do SAFECode.

O SAFECode desenvolveu uma abordagem em três camadas para ajudar os leitores a identificar em qual Grupo de Desenvolvimento (GD) eles se encaixam como uma escala de maturidade para programas de desenvolvimento. Os três níveis de CIS IG usados nas medidas de segurança inspiraram sua abordagem para os DGs abaixo:

Grupo de Desenvolvimento 1

A empresa depende amplamente de software de prateleira ou Open Source (OSS) e pacotes com apenas a adição ocasional de pequenas aplicações ou codificação de sites. A empresa é capaz de aplicar as melhores práticas operacionais e processuais básicas e de gerenciar a segurança de seu software fornecido pelo fornecedor como resultado do cumprimento das orientações dos Controles CIS.

Grupo de Desenvolvimento 2

A empresa depende de alguns aplicações da web e/ou de código nativo personalizados (internos ou desenvolvidos por contratados) integrados com componentes de terceiros e executados no site local ou na nuvem. A empresa possui uma equipe de desenvolvimento que aplica as melhores práticas de desenvolvimento de software. A empresa está atenta à qualidade e manutenção do código aberto de terceiros ou código comercial do qual depende.

Grupo de Desenvolvimento 3

A empresa faz um grande investimento em software personalizado de que necessita para administrar seus negócios e atender seus clientes. Ela pode hospedar software em sua própria infraestrutura, na nuvem ou em ambos, e pode integrar uma grande variedade de componentes de software comercial e de código aberto de terceiros. Fornecedores de software e empresas que oferecem SaaS devem considerar o Grupo de Desenvolvimento 3 como um conjunto mínimo de requisitos.

A primeira etapa no desenvolvimento de um programa de segurança de aplicação é implementar um processo de gestão de vulnerabilidades. Esse processo deve ser integrado ao ciclo de vida de desenvolvimento e deve ser leve para ser inserido no progresso padrão de correção de bugs. O processo deve incluir a análise da causa raiz para corrigir as falhas subjacentes a fim de reduzir as vulnerabilidades futuras e uma classificação de gravidade para priorizar os esforços de correção.

Os desenvolvedores precisam ser treinados em conceitos de segurança de aplicações e práticas de codificação seguras. Isso inclui um processo para adquirir ou avaliar software, módulos e bibliotecas de terceiros usados na aplicação para garantir que eles não apresentem falhas de segurança. Os desenvolvedores devem ser ensinados sobre quais tipos de módulos podem usar com segurança, onde podem ser adquiridos com segurança e quais componentes eles podem ou não devem desenvolver (por exemplo, criptografia).

Fraquezas na infraestrutura que oferece suporte a esses aplicações podem apresentar riscos. Os Controles CIS e o conceito de minimizar a superfície de ataque podem ajudar a proteger redes, sistemas e contas que são usadas nas aplicações. Orientações específicas podem ser encontradas nos Controles CIS 1-7, 12 e 13.

O programa de segurança de aplicação ideal é aquele que introduz a segurança o mais cedo possível no ciclo de vida de desenvolvimento do software. A gestão de problemas de segurança deve ser consistente e integrada à gestão padrão de falhas/bugs de software, ao contrário de um processo separado que compete por recursos de desenvolvimento. Equipes de desenvolvimento maiores ou mais maduras devem considerar a prática da modelagem de ameaças na fase de design. Vulnerabilidades em nível de design são menos comuns do que vulnerabilidades em nível de código; no entanto, elas geralmente são muito graves e muito mais difíceis de consertar rapidamente. A modelagem de ameaças é o processo de identificar e abordar as falhas de design de segurança da aplicação antes que o código seja criado. A modelagem de ameaças requer treinamento específico, conhecimento técnico e de negócios. É mais bem conduzida por meio de “campeões de segurança” internos em cada equipe de desenvolvimento, para liderar as práticas de modelagem de ameaças para o software dessa equipe. Ele também fornece um contexto valioso para atividades downstream, como análise de causa raiz e teste de segurança.

Equipes de desenvolvimento maiores, ou comerciais, também podem considerar um programa de recompensa por bug, onde indivíduos são pagos para encontrar falhas em seus aplicações. Esse programa é mais bem usado para complementar um processo de desenvolvimento seguro interno e pode fornecer um mecanismo eficiente para identificar as classes de vulnerabilidades nas quais o processo precisa se concentrar.

Finalmente, em 2020, o NIST® publicou seu Secure Software Development Framework (SSDF), que reuniu o que a indústria aprendeu sobre segurança de software nas últimas duas décadas e criou uma estrutura de desenvolvimento de software segura para planejar, avaliar e comunicar sobre atividades de segurança de software. As empresas que adquirem software ou serviços podem usar esta estrutura para construir seus requisitos de segurança e entender se o processo de desenvolvimento de um provedor de software segue as melhores práticas.

Estes são alguns recursos de segurança de aplicação:

- **SAFECode Application Security Addendum:** https://safecode.org/cis-controls/
- **NIST® SSDF:** https://csrc.nist.gov/News/2020/mitigating-risk-of-software-vulns-ssdf
- **The Software Alliance:** https://www.bsa.org/reports/updated-bsa-framework-for-secure-software
- **OWASP®:** https://owasp.org/

Medidas de Segurança

MEDIDAS DE SEGURANÇA	TÍTULO DA MEDIDA DE SEGURANÇA/ DESCRIÇÃO DA MEDIDA DE SEGURANÇA	TIPO DE ATIVO	FUNÇÃO DE SEGURANÇA	IG1	IG2	IG3
16.1	**Estabelecer e manter um processo seguro de desenvolvimento de aplicações** Estabeleça e mantenha um processo seguro de desenvolvimento de aplicações. No processo, trate de itens como: padrões de design de aplicação seguro, práticas de codificação seguras, treinamento de desenvolvedor, gestão de vulnerabilidade, segurança de código de terceiros e procedimentos de teste de segurança de aplicação. Revise e atualize a documentação anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.	Aplicações	Proteger		●	●
16.2	**Estabelecer e manter um processo para aceitar e endereçar vulnerabilidades de software** Estabelecer e manter um processo para aceitar e endereçar relatórios de vulnerabilidades de software, incluindo um meio para que as entidades externas relatem. O processo deve incluir itens como: uma política de tratamento de vulnerabilidade que identifica o processo de relatar, a parte responsável por lidar com os relatórios de vulnerabilidade e um processo de entrada, atribuição, correção e teste de correção. Como parte do processo, use um sistema de rastreamento de vulnerabilidade que inclua classificações de gravidade e métricas para medir o tempo de identificação, análise e correção de vulnerabilidades. Revise e atualize a documentação anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança. Os terceiros desenvolvedores de aplicações precisam considerar esta política para o exterior que ajuda a definir as expectativas para as partes interessadas externas.	Aplicações	Proteger		●	●
16.3	**Executar análise de causa raiz em vulnerabilidades de segurança** Execute a análise de causa raiz em vulnerabilidades de segurança. Ao revisar as vulnerabilidades, a análise da causa raiz é a tarefa de avaliar os problemas subjacentes que criam vulnerabilidades no código e permite que as equipes de desenvolvimento vão além de apenas corrigir vulnerabilidades individuais conforme elas surgem.	Aplicações	Proteger		●	●
16.4	**Estabelecer e gerenciar um inventário de componentes de software de terceiros** Estabeleça e gerencie um inventário atualizado de componentes de terceiros usados no desenvolvimento, geralmente chamados de "lista de materiais", bem como componentes programados para uso futuro. Este inventário deve incluir quaisquer riscos que cada componente de terceiros possa representar. Avalie a lista pelo menos uma vez por mês para identificar quaisquer mudanças ou atualizações nesses componentes e valide se o componente ainda é compatível.	Aplicações	Proteger		●	●
16.5	**Usar componentes de software de terceiros atualizados e confiáveis** Use componentes de software de terceiros atualizados e confiáveis. Quando possível, escolha bibliotecas e estruturas estabelecidas e comprovadas que forneçam segurança adequada. Adquira esses componentes de fontes confiáveis ou avalie o software quanto a vulnerabilidades antes de usá-los.	Aplicações	Proteger		●	●

MEDIDAS DE SEGURANÇA	TÍTULO DA MEDIDA DE SEGURANÇA/ DESCRIÇÃO DA MEDIDA DE SEGURANÇA	TIPO DE ATIVO	FUNÇÃO DE SEGURANÇA	IG1	IG2	IG3
16.6	**Estabelecer e manter um sistema de classificação de gravidade e processo para vulnerabilidades de aplicações** Estabeleça e mantenha um sistema de classificação de gravidade e processo para vulnerabilidades de aplicações que facilitem a priorização da ordem em que as vulnerabilidades descobertas são corrigidas. Esse processo inclui a definição de um nível mínimo de aceitabilidade de segurança para a liberação de código ou aplicações. As classificações de gravidade trazem uma forma sistemática de triagem de vulnerabilidades que melhora o gestão de riscos e ajuda a garantir que os bugs mais graves sejam corrigidos primeiro. Revise e atualize o sistema e processo anualmente.	Aplicações	Proteger		●	●
16.7	**Usar modelos de configurações de segurança padrão para infraestrutura de aplicações** Use modelos de configuração de segurança padrão recomendados pelo setor para componentes de infraestrutura de aplicações. Isso inclui servidores subjacentes, bancos de dados e servidores web e se aplica a contêineres de nuvem, componentes de Platform as a Service (PaaS) e componentes de SaaS. Não permita que o software desenvolvido internamente enfraqueça as configurações de segurança.	Aplicações	Proteger		●	●
16.8	**Separar sistemas de produção e não produção** Mantenha ambientes separados para sistemas de produção e não produção.	Aplicações	Proteger		●	●
16.9	**Treinar desenvolvedores em conceitos de segurança de aplicações e codificação segura** Certifique-se de que todo o pessoal de desenvolvimento de software receba treinamento para escrever código seguro para seu ambiente de desenvolvimento e responsabilidades específicas. O treinamento pode incluir princípios gerais de segurança e práticas padrão de segurança de aplicações. Conduza o treinamento pelo menos uma vez por ano e projete de forma a promover a segurança dentro da equipe de desenvolvimento e construir uma cultura de segurança entre os desenvolvedores.	Aplicações	Proteger		●	●
16.10	**Aplicar princípios de design seguro em arquiteturas de aplicações** Aplique princípios de design seguro em arquiteturas de aplicações. Os princípios de design seguro incluem o conceito de privilégio mínimo e aplicação de mediação para validar cada operação que o usuário faz, promovendo o conceito de "nunca confiar nas entradas do usuário". Os exemplos incluem garantir que a verificação explícita de erros seja realizada e documentada para todas as entradas, incluindo tamanho, tipo de dados e intervalos ou formatos aceitáveis. O design seguro também significa minimizar a superfície de ataque da infraestrutura da aplicação, como desligar portas e serviços desprotegidos, remover programas e arquivos desnecessários e renomear ou remover contas padrão.	Aplicações	Proteger		●	●
16.11	**Aproveitar os módulos ou serviços controlados para componentes de segurança de aplicações** Aproveite os módulos ou serviços controlados para os componentes de segurança da aplicação, como gestão de identidade, criptografia e auditoria e log. O uso de recursos da plataforma em funções críticas de segurança reduzirá a carga de trabalho dos desenvolvedores e minimizará a probabilidade de erros de design ou implementação. Os sistemas operacionais modernos fornecem mecanismos eficazes para identificação, autenticação e autorização e disponibilizam esses mecanismos para as aplicações. Use apenas algoritmos de criptografia padronizados, atualmente aceitos e amplamente revisados. Os sistemas operacionais também fornecem mecanismos para criar e manter logs de auditoria seguros.	Aplicações	Proteger		●	●
16.12	**Implementar verificações de segurança em nível de código** Aplique ferramentas de análise estáticas e dinâmicas dentro do ciclo de vida da aplicação para verificar se as práticas de codificação seguras estão sendo seguidas.	Aplicações	Proteger			●
16.13	**Realizar teste de invasão de aplicação** Realize teste de invasão das aplicações. Para aplicações críticas, o teste de invasão autenticado é mais adequado para localizar vulnerabilidades de lógica de negócios do que a varredura de código e o teste de segurança automatizado. O teste de invasão depende da habilidade do testador para manipular manualmente um aplicação como um usuário autenticado e não autenticado.	Aplicações	Proteger			●
16.14	**Conduzir aplicações de modelagem de ameaças** Conduza a modelagem de ameaças. A modelagem de ameaças é o processo de identificar e abordar as falhas de design de segurança da aplicação em um design, antes que o código seja criado. É conduzido por pessoas especialmente treinadas que avaliam o design da aplicação e medem os riscos de segurança para cada ponto de entrada e nível de acesso. O objetivo é mapear a aplicação, a arquitetura e a infraestrutura de uma forma estruturada para entender seus pontos fracos.	Aplicações	Proteger			●

CONTROLE 17

Gestão de respostas a incidentes

SAFEGUARDS TOTAL	9	IG1	3/9	IG2	8/9	IG3	9/9

Visão geral

Estabelecer um programa 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.

Por que este controle é crítico?

Um programa abrangente de segurança cibernética inclui proteções, detecções, resposta e recursos de recuperação. Frequentemente, os dois últimos são esquecidos em empresas imaturas, ou a técnica de resposta a sistemas comprometidos é apenas reconstruí-los ao estado original e seguir em frente. O objetivo principal da resposta a incidentes é identificar ameaças na empresa, responder a elas antes que possam se espalhar e remediá-las antes que possam causar danos. Sem entender todo o escopo de um incidente, como aconteceu e o que pode ser feito para evitar que aconteça novamente, os defensores ficarão em um padrão perpétuo de "acerte a toupeira".

Não podemos esperar que nossas proteções sejam eficazes 100% do tempo. Quando ocorre um incidente, se uma empresa não tem um plano documentado—mesmo com boas pessoas—é quase impossível saber os procedimentos de investigação corretos, relatórios, coleta de dados, responsabilidade de gestão, protocolos legais e estratégia de comunicação que permitirão a empresa entender, gerenciar e recuperar com sucesso.

Junto com a detecção, contenção e erradicação, a comunicação com as partes interessadas é fundamental. Se quisermos reduzir a probabilidade de impacto material devido a um evento cibernético, a liderança da empresa deve saber qual o impacto potencial que pode haver, para que possam ajudar a priorizar as decisões de remediação ou restauração que melhor apoiem a empresa. Essas decisões de negócios podem ser baseadas em conformidade regulatória, regras de divulgação, acordos de nível de serviço com parceiros ou clientes, receita ou impactos de missão.

O tempo de espera desde o momento em que um ataque acontece até o momento em que ele é identificado pode ser dias, semanas ou meses. Quanto mais tempo os atacantes ficam na infraestrutura da empresa, mais incorporados se tornam e irão desenvolver mais maneiras de manter o acesso persistente para quando forem eventualmente descobertos. Com o surgimento do ransomware, que é um gerador de dinheiro estável para os atacantes, esse tempo de permanência é crítico, especialmente com táticas modernas de roubo de dados antes de criptografá-los para resgate.

Procedimentos e ferramentas

Mesmo que uma empresa não tenha recursos para conduzir a resposta a incidentes, ainda é fundamental ter um plano. Isso deveria incluir as fontes de proteções e detecções, uma lista de a quem recorrer para obter assistência e planos de comunicação sobre como transmitir informações à liderança, funcionários, reguladores, parceiros e clientes.

Depois de definir os procedimentos de resposta a incidentes, a equipe de resposta a incidentes, ou um terceiro, deve se envolver em treinamento periódico baseado em cenários, trabalhando em uma série de cenários de ataque ajustados para as ameaças e impactos potenciais que a empresa enfrenta. Esses cenários ajudam a garantir que a liderança corporativa e os membros da equipe técnica entendam sua função no processo de resposta a incidentes para ajudar a prepará-los para lidar com incidentes. É inevitável que os cenários de exercício e treinamento identifiquem lacunas nos planos e processos, e dependências inesperadas, que podem então ser atualizadas no plano.

Empresas mais maduras devem incluir inteligência sobre ameaças e/ou caça a ameaças em seu processo de resposta a incidentes. Isso ajudará a equipe a se tornar mais proativa, identificando atacantes chave ou principais para sua empresa ou indústria a fim de monitorar ou pesquisar seus TTPs. Isso ajudará a focar as detecções e definir procedimentos de resposta para identificar e corrigir mais rapidamente.

As ações no Controle CIS 17 fornecem etapas específicas de alta prioridade que podem melhorar a segurança da empresa e devem fazer parte de qualquer plano abrangente de incidente e resposta. Além disso, recomendamos o seguinte recurso dedicado a este tópico:

- **Council of Registered Security Testers (CREST) Cyber Security Incident Response Guide—CREST fornece orientação, padrões e conhecimento sobre uma ampla variedade de tópicos de defesa cibernética:** https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf.

Medidas de Segurança

MEDIDAS DE SEGURANÇA	TÍTULO DA MEDIDA DE SEGURANÇA/ DESCRIÇÃO DA MEDIDA DE SEGURANÇA	TIPO DE ATIVO	FUNÇÃO DE SEGURANÇA	IG1	IG2	IG3
17.1	**Designar Pessoal para Gerenciar Tratamento de Incidentes** Designe uma pessoa-chave e pelo menos uma backup para gerenciar o processo de tratamento de incidentes da empresa. A equipe de gestão é responsável pela coordenação e documentação dos esforços de resposta e recuperação a incidentes e pode consistir em funcionários internos da empresa, fornecedores terceirizados ou uma abordagem híbrida. Se estiver usando um fornecedor terceirizado, designe pelo menos uma pessoa interna da empresa para supervisionar qualquer trabalho terceirizado. Revise anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.	N/A	Responder	●	●	●
17.2	**Estabelecer e manter informações de contato para relatar incidentes de segurança** Estabeleça e mantenha as informações de contato das partes que precisam ser informadas sobre os incidentes de segurança. Os contatos podem incluir funcionários internos, fornecedores terceirizados, policiais, provedores de seguros cibernéticos, agências governamentais relevantes, parceiros do Information Sharing and Analysis Center (ISAC) ou outras partes interessadas. Verifique os contatos anualmente para garantir que as informações estejam atualizadas.	N/A	Responder	●	●	●
17.3	**Estabelecer e manter um processo corporativo para relatar incidentes** Estabeleça e mantenha um processo corporativo para a força de trabalho relatar incidentes de segurança. O processo inclui cronograma de relatórios, pessoal para relatar, mecanismo para relatar e as informações mínimas a serem relatadas. Certifique-se de que o processo esteja publicamente disponível para toda a força de trabalho. Revise anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.	N/A	Responder	●	●	●
17.4	**Estabelecer e manter um processo de resposta a incidentes** Estabeleça e mantenha um processo de resposta a incidentes que aborde funções e responsabilidades, requisitos de conformidade e um plano de comunicação. Revise anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.	N/A	Responder		●	●
17.5	**Atribuir funções e responsabilidades chave** Atribua funções e responsabilidades chave para resposta a incidentes, incluindo equipe jurídica, TI, segurança da informação, instalações, relações públicas, recursos humanos, respondentes a incidentes e analistas, conforme aplicável. Revise anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.	N/A	Responder		●	●
17.6	**Definir mecanismos de comunicação durante a resposta a incidente** Determine quais mecanismos primários e secundários serão usados para se comunicar e relatar durante um incidente de segurança. Os mecanismos podem incluir ligações, e-mails ou cartas. Lembre-se de que certos mecanismos, como e-mails, podem ser afetados durante um incidente de segurança. Revise anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.	N/A	Responder		●	●
17.7	**Conduzir exercícios de resposta a incidentes rotineiros** Planeje e conduza exercícios de resposta a incidentes rotineiros e cenários para o pessoal-chave envolvido no processo de resposta a incidentes para se preparar para responder a incidentes do mundo real. Os exercícios precisam testar os canais de comunicação, tomada de decisão e fluxos de trabalho. Realize testes anualmente, no mínimo.	N/A	Recuperar		●	●
17.8	**Conduzir análises pós-incidente** Realize análises pós-incidente. As análises pós-incidente ajudam a prevenir a recorrência do incidente por meio da identificação de lições aprendidas e ações de acompanhamento.	N/A	Recuperar		●	●
17.9	**Estabelecer e manter limites de incidentes de segurança** Estabeleça e mantenha limites de incidentes de segurança, incluindo, no mínimo, a diferenciação entre um incidente e um evento. Os exemplos podem incluir: atividade anormal, vulnerabilidade de segurança, fraqueza de segurança, violação de dados, incidente de privacidade, etc. Revise anualmente ou quando ocorrerem mudanças corporativas significativas que possam impactar esta medida de segurança.	N/A	Recuperar			●

CONTROLE 18

Testes de invasão

SAFEGUARDS TOTAL	5	IG1	0/5	IG2	3/5	IG3	5/5

Visão geral

Teste a eficácia e a resiliência dos ativos corporativos por meio da identificação e exploração de fraquezas nos controles (pessoas, processos e tecnologia) e da simulação dos objetivos e ações de um atacante.

Por que este controle é crítico?

Uma postura defensiva bem-sucedida requer um programa abrangente de políticas e governança eficazes, fortes defesas técnicas, combinadas com a ação apropriada das pessoas. No entanto, raramente é perfeito. Em um ambiente complexo onde a tecnologia está em constante evolução e novas técnicas dos atacantes aparecem regularmente, as empresas devem testar periodicamente seus controles para identificar lacunas e avaliar sua resiliência. Este teste pode ser da perspectiva de rede externa, rede interna, aplicação, sistema ou dispositivo. Pode incluir engenharia social de usuários ou desvios de controle de acesso físico.

Muitas vezes, os testes de invasão são realizados para fins específicos:

- Como uma demonstração "dramática" de um ataque, geralmente para convencer os tomadores de decisão das fraquezas de sua empresa
- Como um meio de testar o funcionamento correto das defesas da empresa ("verificação")
- Para testar se a empresa construiu as defesas certas em primeiro lugar ("validação")

Os testes de invasão independentes podem fornecer percepções valiosas e objetivas sobre a existência de vulnerabilidades em ativos corporativos e humanos, e a eficácia das defesas e controles de mitigação para proteger contra impactos adversos para a empresa. Eles fazem parte de um programa abrangente e contínuo de gestão e aprimoramento de segurança. Eles também podem revelar fraquezas do processo, como gestão de configuração ou treinamento do usuário final incompletos ou inconsistentes.

O teste de invasão difere do teste de vulnerabilidade, descrito no Controle CIS7. O teste de vulnerabilidade apenas verifica a presença de ativos corporativos conhecidos e inseguros e para por aí. O teste de invasão vai além para explorar essas fraquezas para ver até onde um atacante pode chegar e quais processos de negócios ou dados podem ser afetados pela exploração dessa vulnerabilidade. Este é um detalhe importante, e muitas vezes o teste de invasão e o teste de vulnerabilidade são usados indevidamente de maneira incorreta. O teste de vulnerabilidade é exclusivamente a varredura automatizada, às vezes com validação manual de falsos positivos, ao passo que o teste de invasão requer mais envolvimento e análise humana, às vezes com suporte por meio do uso de ferramentas ou scripts personalizados. No entanto, o teste de vulnerabilidade geralmente é um ponto de partida para um teste de invasão.

Outro termo comum são exercícios de "Red Team". Eles são semelhantes aos testes de invasão em que as vulnerabilidades são exploradas; no entanto, a diferença é o foco. Os Red Teams simulam TTPs de atacantes específicos para avaliar como o ambiente de uma empresa resistiria a um ataque de um adversário específico ou uma categoria de adversários.

Procedimentos e ferramentas

O teste de invasão começa com o reconhecimento da empresa e do ambiente, e varredura para identificar as vulnerabilidades que podem ser usadas como entradas na empresa. É importante certificar-se de que todos os ativos corporativos que estão dentro do escopo sejam descobertos, e não apenas com base em uma lista estática, que pode estar desatualizada ou incompleta. Em seguida, as vulnerabilidades serão identificadas nesses alvos. Explorações a essas vulnerabilidades são executadas para demonstrar especificamente como um adversário pode subverter as metas de segurança da empresa (por exemplo, a proteção de dados sensíveis específicos) ou alcançar objetivos adversários específicos (por exemplo, o estabelecimento de uma infraestrutura secreta de Comando e Controle (C2)). Os resultados fornecem uma visão mais profunda, por meio de demonstração, dos riscos de negócios de várias vulnerabilidades.

Os testes de invasão são caros, complexos e potencialmente apresentam seus próprios riscos. Pessoas experientes de fornecedores confiáveis devem conduzi-los. Alguns riscos incluem desligamento inesperado de sistemas que podem ser instáveis, explorações que podem excluir ou corromper dados ou configurações e a saída de um relatório de teste que precisa ser protegido, porque fornece instruções passo a passo sobre como invadir a empresa para direcionar ativos ou dados críticos.

Cada empresa deve definir um escopo claro e regras de contratação para o teste de invasão. O escopo de tais projetos deve incluir, no mínimo, ativos corporativos com as informações de maior valor e funcionalidade de processamento de produção. Outros sistemas de valor inferior também podem ser testados para ver se podem ser usados como pontos de pivô para comprometer alvos de valor superior. As regras de contratação para análises de teste de invasão devem descrever, no mínimo, os horários do dia para o teste, a duração do(s) teste(s) e a abordagem geral do teste. Apenas algumas pessoas na empresa devem saber quando um teste de invasão for realizado e um ponto de contato principal na empresa deve ser designado se ocorrerem problemas.

As medidas de segurança neste Controle CIS fornecem etapas específicas de alta prioridade que podem melhorar a segurança da empresa e devem fazer parte de qualquer teste de invasão. Além disso, recomendamos o uso de alguns dos excelentes recursos abrangentes dedicados a este tópico para apoiar o planejamento, gestão e relatórios de teste de segurança:

- **OWASP Penetration Testing Methodologies:** https://www.owasp.org/index.php/Penetration_testing_methodologies
- **PCI Security Standards Council:** https://www.pcisecuritystandards.org/documents/Penetration-Testing-Guidance-v1_1.pdf

Medidas de Segurança

MEDIDAS DE SEGURANÇA	TÍTULO DA MEDIDA DE SEGURANÇA/ DESCRIÇÃO DA MEDIDA DE SEGURANÇA	TIPO DE ATIVO	FUNÇÃO DE SEGURANÇA	IG1	IG2	IG3
18.1	**Estabelecer e manter um programa de teste de invasão** Estabeleça e mantenha um programa de teste de invasão adequado ao tamanho, complexidade e maturidade da empresa. As características do programa de teste de invasão incluem escopo, como rede, aplicação web, Application Programming Interface (API), serviços hospedados e controles de instalações físicas; frequência; limitações, como horas aceitáveis e tipos de ataque excluídos; informações do ponto de contato; remediação, por exemplo, como as descobertas serão encaminhadas internamente; e requisitos retrospectivos.	N/A	Identificar		●	●
18.2	**Realizar testes de invasão externos periódicos** Realize testes de invasão externos periódicos com base nos requisitos do programa, pelo menos uma vez por ano. O teste de invasão externo deve incluir reconhecimento empresarial e ambiental para detectar informações exploráveis. O teste de invasão requer habilidades e experiência especializadas e deve ser conduzido por uma parte qualificada. O teste pode ser clear box ou opaque box.	Rede	Identificar		●	●
18.3	**Corrigir as descobertas do teste de invasão** Corrija as descobertas do teste de invasão com base na política da empresa para o escopo e a priorização da correção.	Rede	Proteger		●	●
18.4	**Validar as Medidas de Segurança** Valide as medidas de segurança após cada teste de invasão. Se necessário, modifique os conjuntos de regras e recursos para detectar as técnicas usadas durante o teste.	Rede	Proteger			●
18.5	**Realizar testes de invasão internos periódicos** Realize testes de invasão internos periódicos com base nos requisitos do programa, pelo menos uma vez por ano. O teste pode ser clear box ou opaque box.	N/A	Identificar			●

APÊNDICE A

Recursos e Referências

CIS Benchmarks™ Program: http://www.cisecurity.org/cis-benchmarks/

CIS Controls Cloud Companion Guide: https://www.cisecurity.org/controls/v8/

CIS Community Defense Model (CDM): https://www.cisecurity.org/controls/v8/

CIS Configuration Assessment Tool (CIS-CAT®): https://learn.cisecurity.org/cis-cat-lite

CIS Controls Assessment Specification: https://controls-assessment-specification.readthedocs.io/en/stable/about/cas.html

CIS Controls Implementation Groups: https://www.cisecurity.org/controls/v8/

CIS Controls Industrial Control Systems Implementation Guide: https://www.cisecurity.org/controls/v8/

CIS Controls Internet of Things Companion Guide: https://www.cisecurity.org/controls/v8/

CIS Controls Mobile Companion Guide: https://www.cisecurity.org/controls/v8/
CIS Risk Assessment Method (RAM): https://www.cisecurity.org/controls/v8/

CIS Controls Self Assessment Tool (CSAT): https://www.cisecurity.org/blog/cis-csat-free-tool-assessing-implementation-of-cis-controls/

CIS Controls Telework and Small Office Network Security Guide: https://www.cisecurity.org/controls/v8/

CIS Password Policy Guide: https://www.cisecurity.org/white-papers/cis-password-policy-guide/

Cloud Security Alliance (CSA): https://cloudsecurityalliance.org/

Council of Registered Security Testers (CREST) Cyber Security Incident Response Guide: CREST provides guidance, standards, and knowledge on a wide variety of cyber defense topics: https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf

EDUCAUSE: https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/awareness-campaigns

International Organization for Standardization: https://www.iso.org/home.html

National Cyber Security Centre (U.K.): https://www.ncsc.gov.uk/guidance/10-steps-user-education-and-awareness

National Institute of Standards and Technology (NIST®): https://www.nist.gov/

National Institute of Standards and Technology (NIST®) SSDF: https://csrc.nist.gov/News/2020/mitigating-risk-of-software-vulns-ssdf

National Institute of Standards and Technology (NIST®) National Checklist Program Repository: https://nvd.nist.gov/ncp/repository

National Institute of Standards and Technology (NIST®) Digital Identity Guidelines: https://pages.nist.gov/800-63-3/

National Institute of Standards and Technology (NIST®) FIPS 140-2: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf

National Institute of Standards and Technology (NIST®) FIPS 140-3: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf

National Institute of Standards and Technology (NIST®) SP 800-50 Infosec Awareness Training: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf

National Institute of Standards and Technology (NIST®) SP 800-88r1 – Guidelines for Media Sanitization: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

National Cyber Security Alliance (NCSA): https://staysafeonline.org/

OWASP®: https://owasp.org/

OWASP® Penetration Testing Methodologies: https://www.owasp.org/index.php/Penetration_testing_methodologies

PCI Security Standards Council: https://www.pcisecuritystandards.org/documents/Penetration-Testing-Guidance-v1_1.pdf

SANS: https://www.sans.org/security-awareness-training/resources

SAFECode Application Security Addendum: https://safecode.org/cis-controls/

National Institute of Standards and Technology (NIST®) SP 800-126r3 The Technical Specification for the Security Content Automation Protocol (SCAP): https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-126r3.pdf

The Software Alliance: https://www.bsa.org/reports/updated-bsa-framework-for-secure-software

Verizon Data Breach Investigations Report: https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

APÊNDICE B

Controls and Safeguards Index

CONTROLE 01 / SEGURANÇA 1.1 — CONTROLE 02 / SEGURANÇA 2.1

CONTROLE	MEDIDAS DE SEGURANÇA	TÍTULO DA MEDIDA DE SEGURANÇA/ DESCRIÇÃO DA MEDIDA DE SEGURANÇA	TIPO DE ATIVO	FUNÇÃO DE SEGURANÇA	IG1	IG2	IG3
01		**Inventário e controle de ativos corporativos** Gestão ativa (inventariar, rastrear e corrigir) de todos os ativos corporativos (dispositivos de usuário final, incluindo portáteis e móveis; dispositivos de rede; dispositivos não computacionais; Internet das Coisas (IoT); e servidores) conectados fisicamente à infraestrutura, virtualmente, remotamente, e aqueles em ambientes de nuvem, para saber com precisão a totalidade dos ativos que precisam ser monitorados e protegidos dentro da empresa. Isso também ajudará na identificação de ativos não autorizados e não gerenciados para removê-los ou remediá-los.						
	1.1	**Estabelecer e manter um inventário detalhado de ativos corporativos** Estabeleça e mantenha um inventário preciso, detalhado e atualizado de todos os ativos corporativos com potencial para armazenar ou processar dados, incluindo: dispositivos de usuário final (incluindo portáteis e móveis), dispositivos de rede, dispositivos não computacionais/IoT e servidores. Certifique-se de que o inventário registre o endereço de rede (se estático), endereço de hardware, nome da máquina, proprietário do ativo de dados, departamento para cada ativo e se o ativo foi aprovado para se conectar à rede. Para dispositivos móveis de usuário final, as ferramentas do tipo MDM podem oferecer suporte a esse processo, quando apropriado. Este inventário inclui ativos conectados à infraestrutura fisicamente, virtualmente, remotamente e aqueles dentro dos ambientes de nuvem. Além disso, inclui ativos que são regularmente conectados à infraestrutura de rede corporativa, mesmo que não estejam sob o controle da empresa. Revise e atualize o inventário de todos os ativos corporativos semestralmente ou com mais frequência.	Dispositivo	Identificar	●	●	●
	1.2	**Endereçar ativos não autorizados** Assegure que exista um processo para lidar com ativos não autorizados semanalmente. A empresa pode escolher remover o ativo da rede, negar que o ativo se conecte remotamente à rede ou colocar o ativo em quarentena.	Dispositivo	Responder	●	●	●
	1.3	**Usar uma ferramenta de descoberta ativa** Utilize uma ferramenta de descoberta ativa para identificar ativos conectados à rede corporativa. Configure a ferramenta de descoberta ativa para executar diariamente ou com mais frequência.	Dispositivo	Detectar		●	●
	1.4	**Usar o Dynamic Host Configuration Protocol (DHCP) para atualizar o inventário de ativos corporativos** Use o log do DHCP em todos os servidores DHCP ou ferramentas de gestão de endereço Internet Protocol (IP) para atualizar o inventário de ativos corporativos. Revise e use logs para atualizar o inventário de ativos corporativos semanalmente ou com mais frequência.	Dispositivo	Identificar		●	●
	1.5	**Usar uma ferramenta de descoberta passiva** Use uma ferramenta de descoberta passiva para identificar ativos conectados à rede corporativa. Revise e use varreduras para atualizar o inventário de ativos corporativos pelo menos semanalmente ou com mais frequência.	Dispositivo	Detectar			●
02		**Inventário e controle de ativos de software** Gestão ativa (inventariar, rastrear e corrigir) de todos os softwares (sistemas operacionais e aplicações) na rede para que apenas o software autorizado seja instalado e possa ser executado, e que o software não autorizado e não gerenciado seja encontrado e impedido de ser instalado ou executado.					
	2.1	**Estabelecer e manter um inventário de software** Estabeleça e mantenha um inventário detalhado de todos os softwares licenciados instalados em ativos corporativos. O inventário de software deve documentar o título, editor, data inicial de instalação/uso e objetivo de negócio de cada entrada; quando apropriado, inclua o Uniform Resource Locator(URL), app store(s), versão(ões), mecanismo de implantação e data de desativação. Revise e atualize o inventário de software semestralmente ou com mais frequência.	Aplicações	Identificar	●	●	●

CONTROLE	MEDIDAS DE SEGURANÇA	TÍTULO DA MEDIDA DE SEGURANÇA/ DESCRIÇÃO DA MEDIDA DE SEGURANÇA	TIPO DE ATIVO	FUNÇÃO DE SEGURANÇA	IG1	IG2	IG3
	2.2	**Assegurar que o software autorizado seja atualmente suportado** Assegure que apenas software atualmente suportado seja designado como autorizado no inventário de software para ativos corporativos. Se o software não é suportado, mas é necessário para o cumprimento da missão da empresa, documente uma exceção detalhando os controles de mitigação e a aceitação do risco residual. Para qualquer software não suportado sem uma documentação de exceção, designe como não autorizado. Revise o inventário de software para verificar o suporte do software pelo menos uma vez por mês ou com mais frequência.	Aplicações	Identificar	●	●	●
	2.3	**Endereçar o software não autorizado** Assegure que o software não autorizado seja retirado de uso em ativos corporativos ou receba uma exceção documentada. Revise mensalmente ou com mais frequência	Aplicações	Responder	●	●	●
	2.4	**Utilizar ferramentas automatizadas de inventário de software** Utilize ferramentas de inventário de software, quando possível, em toda a empresa para automatizar a descoberta e documentação do software instalado	Aplicações	Detectar		●	●
	2.5	**Lista de permissões de Software autorizado** Use controles técnicos, como a lista de permissões de aplicações, para garantir que apenas o software autorizado possa ser executado ou acessado. Reavalie semestralmente ou com mais frequência.	Aplicações	Proteger		●	●
	2.6	**Lista de permissões de bibliotecas autorizadas** Use os controles técnicos para garantir que apenas as bibliotecas de software autorizadas, como arquivos .dll, .ocx, .so, etc. específicos, tenham permissão para carregar em um processo do sistema. Impedir que bibliotecas não autorizadas sejam carregadas em um processo do sistema. Reavalie semestralmente ou com mais frequência.	Aplicações	Proteger		●	●
	2.7	**Lista de permissões de Scripts autorizados** Use controles técnicos, como assinaturas digitais e controle de versão, para garantir que apenas scripts autorizados, como arquivos .ps1, .py, etc. específicos, tenham permissão para executar. Bloqueie a execução de scripts não autorizados. Reavalie semestralmente ou com mais frequência.	Aplicações	Proteger			●
03		**Proteção de dados** Desenvolver processos e controles técnicos para identificar, classificar, manusear com segurança, reter e descartar dados.					
	3.1	**Estabelecer e manter um processo de gestão de dados** Estabeleça e mantenha um processo de gestão de dados. No processo, trate a sensibilidade dos dados, o proprietário dos dados, o manuseio dos dados, os limites de retenção de dados e os requisitos de descarte, com base em padrões de sensibilidade e retenção para a empresa. Revise e atualize a documentação anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.	Dados	Identificar	●	●	●
	3.2	**Estabelecer e manter um inventário de dados** Estabeleça e mantenha um inventário de dados, com base no processo de gestão de dados da empresa. No mínimo, inventarie os dados sensíveis. Revise e atualize o inventário anualmente, no mínimo, com prioridade para os dados sensíveis.	Dados	Identificar	●	●	●
	3.3	**Configurar listas de controle de acesso a dados** Configure listas de controle de acesso a dados com base na necessidade de conhecimento do usuário. Aplique listas de controle de acesso a dados, também conhecidas como permissões de acesso, a sistemas de arquivos, bancos de dados e aplicações locais e remotos.	Dados	Proteger	●	●	●
	3.4	**Aplicar retenção de dados** Retenha os dados de acordo com o processo de gestão de dados da empresa. A retenção de dados deve incluir prazos mínimos e máximos.	Dados	Proteger	●	●	●
	3.5	**Descartar dados com segurança** Descarte os dados com segurança conforme descrito no processo de gestão de dados da empresa. Certifique-se de que o processo e o método de descarte sejam compatíveis com a sensibilidade dos dados.	Dados	Proteger	●	●	●

CONTROLE	MEDIDAS DE SEGURANÇA	TÍTULO DA MEDIDA DE SEGURANÇA/ DESCRIÇÃO DA MEDIDA DE SEGURANÇA	TIPO DE ATIVO	FUNÇÃO DE SEGURANÇA	IG1	IG2	IG3
	3.6	**Criptografar dados em dispositivos de usuário final.** Criptografe os dados em dispositivos de usuário final que contenham dados sensíveis. Exemplos de implementações podem incluir: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.	Dispositivo	Proteger	●	●	●
	3.7	**Estabelecer e manter um esquema de classificação de dados** Estabeleça e mantenha um esquema geral de classificação de dados para a empresa. As empresas podem usar rótulos, como "Sensível", "Confidencial" e "Público", e classificar seus dados de acordo com esses rótulos. Revise e atualize o esquema de classificação anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.	Dados	Identificar		●	●
	3.8	**Documentar Fluxos de Dados** Documente fluxos de dados. A documentação do fluxo de dados inclui fluxos de dados do provedor de serviços e deve ser baseada no processo de gestão de dados da empresa. Revise e atualize a documentação anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança	Dados	Identificar		●	●
	3.9	**Criptografar dados em mídia removível** Criptografe os dados em mídia removível.	Dados	Proteger		●	●
	3.10	**Criptografar dados sensíveis em trânsito** Criptografe dados sensíveis em trânsito. Exemplos de implementações podem incluir: Transport Layer Security (TLS) e Open Secure Shell (OpenSSH)	Dados	Proteger		●	●
	3.11	**Criptografar dados sensíveis em repouso** Criptografe dados sensíveis em repouso em servidores, aplicações e bancos de dados que contenham dados sensíveis. A criptografia da camada de armazenamento, também conhecida como criptografia do lado do servidor, atende ao requisito mínimo desta medida de segurança. Métodos de criptografia adicionais podem incluir criptografia de camada de aplicação, também conhecida como criptografia do lado do cliente, onde o acesso ao(s) dispositivo(s) de armazenamento de dados não permite o acesso aos dados em texto simples.	Dados	Proteger		●	●
	3.12	**Segmentar o processamento e o armazenamento de dados com base na sensibilidade** Segmente o processamento e o armazenamento de dados com base na sensibilidade dos dados. Não processe dados sensíveis em ativos corporativos destinados a dados de menor sensibilidade.	Rede	Proteger		●	●
	3.13	**Implantar uma solução de prevenção contra perda de dados** Implementar uma ferramenta automatizada, como uma ferramenta de prevenção de perda de dados (DLP) baseada em host para identificar todos os dados sensíveis armazenados, processados ou transmitidos por meio de ativos corporativos, incluindo aqueles localizados no site local ou em um provedor de serviços remoto, e atualizar o inventário de dados sensíveis da empresa.	Dados	Proteger			●
	3.14	**Registrar o acesso a dados sensíveis** Registre o acesso a dados sensíveis, incluindo modificação e descarte.	Dados	Detectar			●
04		**Configuração segura de ativos corporativos e software** Estabelecer e manter a configuração segura de ativos corporativos (dispositivos de usuário final, incluindo portáteis e móveis; dispositivos de rede; dispositivos não computacionais/IoT; e servidores) e software (sistemas operacionais e aplicações).					
	4.1	**Estabelecer e manter um processo de configuração segura** Estabeleça e mantenha um processo de configuração segura para ativos corporativos (dispositivos de usuário final, incluindo portáteis e móveis; dispositivos não computacionais/IoT; e servidores) e software (sistemas operacionais e aplicações). Revise e atualize a documentação anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.	Aplicações	Proteger	●	●	●
	4.2	**Estabelecer e Manter um Processo de Configuração Segura para a Infraestrutura de Rede** Estabeleça e mantenha um processo de configuração segura para dispositivos de rede. Revise e atualize a documentação anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.	Rede	Proteger	●	●	●

CONTROLE	MEDIDAS DE SEGURANÇA	TÍTULO DA MEDIDA DE SEGURANÇA/ DESCRIÇÃO DA MEDIDA DE SEGURANÇA	TIPO DE ATIVO	FUNÇÃO DE SEGURANÇA	IG1	IG2	IG3
	4.3	**Configurar o bloqueio automático de sessão nos ativos corporativos** Configure o bloqueio automático de sessão nos ativos corporativos após um período definido de inatividade. Para sistemas operacionais de uso geral, o período não deve exceder 15 minutos. Para dispositivos móveis de usuário final, o período não deve exceder 2 minutos.	Usuários	Proteger	●	●	●
	4.4	**Implementar e gerenciar um firewall nos servidores** Implemente e gerencie um firewall nos servidores, onde houver suporte. Exemplos de implementações incluem um firewall virtual, firewall do sistema operacional ou um agente de firewall de terceiros.	Dispositivo	Proteger	●	●	●
	4.5	**Implementar e gerenciar um firewall nos dispositivos de usuário final** Implemente e gerencie um firewall baseado em host ou uma ferramenta de filtragem de porta nos dispositivos de usuário final, com uma regra de negação padrão que bloqueia todo o tráfego, exceto os serviços e portas que são explicitamente permitidos.	Dispositivo	Proteger	●	●	●
	4.6	**Gerenciar com segurança os ativos e software corporativos** Gerencie com segurança os ativos e software corporativos. Exemplos de implementações incluem gestão de configuração por meio de version-controlled-infrastructure-as-code e acesso a interfaces administrativas por meio de protocolos de rede seguros, como Secure Shell (SSH) e Hypertext Transfer Protocol Secure (HTTPS). Não use protocolos de gestão inseguros, como Telnet (Teletype Network) e HTTP, a menos que seja operacionalmente essencial.	Rede	Proteger	●	●	●
	4.7	**Gerenciar contas padrão nos ativos e software corporativos** Gerencie contas padrão nos ativos e software corporativos, como root, administrador e outras contas de fornecedores pré-configuradas. Exemplos de implementações podem incluir: desativar contas padrão ou torná-las inutilizáveis.	Usuários	Proteger	●	●	●
	4.8	**Desinstalar ou desativar serviços desnecessários nos ativos e software corporativos** Desinstale ou desative serviços desnecessários nos ativos e software corporativos, como um serviço de compartilhamento de arquivos não utilizado, módulo de aplicação da web ou função de serviço.	Dispositivo	Proteger		●	●
	4.9	**Configurar servidores DNS confiáveis nos ativos corporativos** Configure servidores DNS confiáveis nos ativos corporativos. As exemplos de implementações incluem: configuração de ativos para usar servidores DNS controlados pela empresa e/ou servidores DNS confiáveis acessíveis externamente.	Dispositivo	Proteger		●	●
	4.10	**Impor o bloqueio automático de dispositivos nos dispositivos portáteis do usuário final** Imponha o bloqueio automático do dispositivo seguindo um limite pré-determinado de tentativas de autenticação local com falha nos dispositivos portáteis de usuário final, quando compatível. Para laptops, não permita mais de 20 tentativas de autenticação com falha; para tablets e smartphones, não mais do que 10 tentativas de autenticação com falha. Exemplos de implementações incluem Microsoft® InTune Device Lock e Apple® Configuration Profile maxFailedAttempts.	Dispositivo	Responder		●	●
	4.11	**Impor a capacidade de limpeza remota nos dispositivos portáteis do usuário final** Limpe remotamente os dados corporativos de dispositivos portáteis de usuário final de propriedade da empresa quando for considerado apropriado, como dispositivos perdidos ou roubados, ou quando um indivíduo não trabalha mais na empresa.	Dispositivo	Proteger		●	●
	4.12	**Separar os Espaços de Trabalho Corporativos nos dispositivos móveis** Certifique-se de que a separação de espaços de trabalho corporativos seja usada nos dispositivos móveis de usuário final, onde houver suporte. Exemplos de implementações incluem o uso de um Apple® Configuration Profile ou Android ™ Work Profile para separar aplicações e dados corporativos de aplicações e dados pessoais.	Dispositivo	Proteger			●

CONTROLE	MEDIDAS DE SEGURANÇA	TÍTULO DA MEDIDA DE SEGURANÇA/ DESCRIÇÃO DA MEDIDA DE SEGURANÇA	TIPO DE ATIVO	FUNÇÃO DE SEGURANÇA	IG1	IG2	IG3
05		**Gestão de contas** Use processos e ferramentas para atribuir e gerenciar autorização de credenciais para contas de usuário, incluindo contas de administrador, bem como contas de serviço, de ativos corporativos e software.					
	5.1	**Estabelecer e manter um inventário de contas** Estabeleça e mantenha um inventário de todas as contas gerenciadas na empresa. O inventário deve incluir contas de usuário e administrador. O inventário, no mínimo, deve conter o nome da pessoa, nome de usuário, datas de início/término e departamento. Valide se todas as contas ativas estão autorizadas, em uma programação recorrente, no mínimo trimestralmente ou com mais frequência.	Usuários	Identificar	●	●	●
	5.2	**Usar senhas exclusivas** Use senhas exclusivas para todos os ativos corporativos. As melhores práticas de implementação incluem, no mínimo, uma senha de 8 caracteres para contas que usam MFA e uma senha de 14 caracteres para contas que não usam MFA.	Usuários	Proteger	●	●	●
	5.3	**Desabilitar contas inativas** Exclua ou desabilite quaisquer contas inativas após um período de 45 dias de inatividade, onde for suportado.	Usuários	Responder	●	●	●
	5.4	**Restringir privilégios de administrador a contas de Administrador dedicadas** Restrinja os privilégios de administrador a contas de administrador dedicadas nos ativos corporativos. Realize atividades gerais de computação, como navegação na Internet, e-mail e uso do pacote de produtividade, a partir da conta primária não privilegiada do usuário.	Usuários	Proteger	●	●	●
	5.5	**Estabelecer e manter um inventário de contas de serviço** Estabeleça e mantenha um inventário de contas de serviço. O inventário, no mínimo, deve conter departamento proprietário, data de revisão e propósito. Realize análises de contas de serviço para validar se todas as contas ativas estão autorizadas, em uma programação recorrente, no mínimo trimestralmente ou com mais frequência.	Usuários	Identificar		●	●
	5.6	**Centralizar a gestão de contas** Centralize a gestão de contas por meio de serviço de diretório ou de identidade.	Usuários	Proteger		●	●
06		**Gestão do controle de acesso** Use processos e ferramentas para criar, atribuir, gerenciar e revogar credenciais de acesso e privilégios para contas de usuário, administrador e serviço para ativos e software corporativos.					
	6.1	**Estabelecer um Processo de Concessão de Acesso** Estabeleça e siga um processo, de preferência automatizado, para conceder acesso aos ativos corporativos mediante nova contratação, concessão de direitos ou mudança de função de um usuário.	Usuários	Proteger	●	●	●
	6.2	**Estabelecer um Processo de Revogação de Acesso** Estabeleça e siga um processo, de preferência automatizado, para revogar o acesso aos ativos corporativos, por meio da desativação de contas imediatamente após o encerramento, revogação de direitos ou mudança de função de um usuário. Desativar contas, em vez de excluí-las, pode ser necessário para preservar as trilhas de auditoria.	Usuários	Proteger	●	●	●
	6.3	**Exigir MFA para aplicações expostas externamente** Exija que todas as aplicações corporativas ou de terceiros expostas externamente apliquem o MFA, onde houver suporte. Impor o MFA por meio de um serviço de diretório ou provedor de SSO é uma implementação satisfatória desta medida de segurança	Usuários	Proteger	●	●	●
	6.4	**Exigir MFA para acesso remoto à rede** Exija MFA para acesso remoto à rede.	Usuários	Proteger	●	●	●
	6.5	**Exigir MFA para acesso administrativo** Exija MFA para todas as contas de acesso administrativo, onde houver suporte, em todos os ativos corporativos, sejam gerenciados no site local ou por meio de um provedor terceirizado.	Usuários	Proteger	●	●	●

CONTROLE	MEDIDAS DE SEGURANÇA	TÍTULO DA MEDIDA DE SEGURANÇA/ DESCRIÇÃO DA MEDIDA DE SEGURANÇA	TIPO DE ATIVO	FUNÇÃO DE SEGURANÇA	IG1	IG2	IG3
	6.6	**Estabelecer e manter um inventário de sistemas de autenticação e autorização** Estabeleça e mantenha um inventário dos sistemas de autenticação e autorização da empresa, incluindo aqueles hospedados no site local ou em um provedor de serviços remoto. Revise e atualize o inventário, no mínimo, anualmente ou com mais frequência.	Usuários	Identificar		●	●
	6.7	**Centralizar o controle de acesso** Centralize o controle de acesso para todos os ativos corporativos por meio de um serviço de diretório ou provedor de SSO, onde houver suporte.	Usuários	Proteger		●	●
	6.8	**Definir e manter o controle de acesso baseado em funções** Defina e mantenha o controle de acesso baseado em funções, determinando e documentando os direitos de acesso necessários para cada função dentro da empresa para cumprir com sucesso suas funções atribuídas. Realize análises de controle de acesso de ativos corporativos para validar se todos os privilégios estão autorizados, em uma programação recorrente, no mínimo uma vez por ano ou com maior frequência.	Dados	Proteger			●
07		**Gestão contínua de vulnerabilidades** Desenvolva um plano para avaliar e rastrear vulnerabilidades continuamente em todos os ativos corporativos dentro da infraestrutura da empresa, a fim de remediar e minimizar a janela de oportunidade para atacantes. Monitore fontes públicas e privadas para novas informações sobre ameaças e vulnerabilidades.					
	7.1	**Estabelecer e manter um processo de gestão de vulnerabilidade** Estabeleça e mantenha um processo de gestão de vulnerabilidade documentado para ativos corporativos. Revise e atualize a documentação anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.	Aplicações	Proteger	●	●	●
	7.2	**Estabelecer e manter um processo de remediação** Estabeleça e mantenha uma estratégia de remediação baseada em risco documentada em um processo de remediação, com revisões mensais ou mais frequentes.	Aplicações	Responder	●	●	●
	7.3	**Executar a gestão automatizada de patches do sistema operacional** Realize atualizações do sistema operacional em ativos corporativos por meio da gestão automatizada de patches mensalmente ou com mais frequência.	Aplicações	Proteger	●	●	●
	7.4	**Executar a gestão automatizada de patches de aplicações** Realize atualizações de aplicações em ativos corporativos por meio da gestão automatizada de patches mensalmente ou com mais frequência.	Aplicações	Proteger	●	●	●
	7.5	**Realizar varreduras automatizadas de vulnerabilidade em ativos corporativos internos** Realize varreduras automatizadas de vulnerabilidade em ativos corporativos internos trimestralmente ou com mais frequência. Realize varreduras autenticadas e não autenticadas, usando uma ferramenta de varredura de vulnerabilidade compatível com o SCAP.	Aplicações	Identificar		●	●
	7.6	**Realizar varreduras automatizadas de vulnerabilidade em ativos corporativos expostos externamente** Execute varreduras de vulnerabilidade automatizadas de ativos corporativos expostos externamente usando uma ferramenta de varredura de vulnerabilidade compatível com o SCAP. Execute varreduras mensalmente ou com mais frequência.	Aplicações	Identificar		●	●
	7.7	**Corrigir vulnerabilidades detectadas** Corrija as vulnerabilidades detectadas no software por meio de processos e ferramentas mensalmente, ou mais frequentemente, com base no processo de correção.	Aplicações	Responder		●	●

CONTROLE	MEDIDAS DE SEGURANÇA	TÍTULO DA MEDIDA DE SEGURANÇA/ DESCRIÇÃO DA MEDIDA DE SEGURANÇA	TIPO DE ATIVO	FUNÇÃO DE SEGURANÇA	IG1	IG2	IG3
08		**Gestão de registros de auditoria** Colete, alerte, analise e retenha logs de auditoria de eventos que podem ajudar a detectar, compreender ou se recuperar de um ataque.					
	8.1	**Estabelecer e manter um processo de gestão de log de auditoria** Estabeleça e mantenha um processo de gestão de log de auditoria que defina os requisitos de log da empresa. No mínimo, trate da coleta, revisão e retenção de logs de auditoria para ativos corporativos. Revise e atualize a documentação anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.	Rede	Proteger	●	●	●
	8.2	**Coletar logs de auditoria** Colete logs de auditoria. Certifique-se de que o log, de acordo com o processo de gestão de log de auditoria da empresa, tenha sido habilitado em todos os ativos.	Rede	Detectar	●	●	●
	8.3	**Garantir o armazenamento adequado do registro de auditoria** Certifique-se de que os destinos dos logs mantenham armazenamento adequado para cumprir o processo de gestão de log de auditoria da empresa.	Rede	Proteger	●	●	●
	8.4	**Padronizar a sincronização de tempo** Padronize a sincronização de tempo. Configure pelo menos duas fontes de tempo sincronizadas nos ativos corporativos, onde houver suporte.	Rede	Proteger		●	●
	8.5	**Coletar logs de auditoria detalhados** Configure o log de auditoria detalhado para ativos corporativos contendo dados sensíveis. Inclua a origem do evento, data, nome de usuário, carimbo de data/hora, endereços de origem, endereços de destino e outros elementos úteis que podem ajudar em uma investigação forense.	Rede	Detectar		●	●
	8.6	**Coletar logs de auditoria de consulta dns** Colete logs de auditoria de consulta DNS em ativos corporativos, quando apropriado e suportado.	Rede	Detectar		●	●
	8.7	**Coletar logs de auditoria de requisição de url** Colete logs de auditoria de requisição de URL em ativos corporativos, quando apropriado e suportado.	Rede	Detectar		●	●
	8.8	**Coletar logs de auditoria de linha de comando** Colete logs de auditoria de linha de comando. Exemplos de implementações incluem a coleta de logs de auditoria do PowerShell®, BASH ™ e terminais administrativos remotos.	Dispositivo	Detectar		●	●
	8.9	**Centralizar os logs de auditoria** Centralize, na medida do possível, a coleta e retenção de logs de auditoria nos ativos corporativos.	Rede	Detectar		●	●
	8.10	**Reter os logs de auditoria** Reter os logs de auditoria em ativos corporativos por no mínimo 90 dias.	Rede	Proteger		●	●
	8.11	**Conduzir revisões de log de auditoria** Realize análises de logs de auditoria para detectar anomalias ou eventos anormais que possam indicar uma ameaça potencial. Realize revisões semanalmente ou com mais frequência.	Rede	Detectar		●	●
	8.12	**Colete logs do provedor de serviços** Colete logs do provedor de serviços, onde houver suporte. Exemplos de implementações incluem coleta de eventos de autenticação e autorização, eventos de criação e de descarte de dados e eventos de gestão de usuários.	Dados	Detectar			●

CONTROLE	MEDIDAS DE SEGURANÇA	TÍTULO DA MEDIDA DE SEGURANÇA/ DESCRIÇÃO DA MEDIDA DE SEGURANÇA	TIPO DE ATIVO	FUNÇÃO DE SEGURANÇA	IG1	IG2	IG3
09		**Proteções de e-mail e navegador Web** Melhore as proteções e detecções de vetores de ameaças de e-mail e web, pois são oportunidades para atacantes manipularem o comportamento humano por meio do engajamento direto.					
	9.1	**Garantir o uso apenas de navegadores e clientes de e-mail suportados plenamente** Certifique-se de que apenas navegadores e clientes de e-mail suportados plenamente tenham permissão para executar na empresa, usando apenas a versão mais recente dos navegadores e clientes de e-mail fornecidos pelo fornecedor.	Aplicações	Proteger	●	●	●
	9.2	**Usar serviços de filtragem de DNS** Use os serviços de filtragem de DNS em todos os ativos corporativos para bloquear o acesso a domínios mal-intencionados conhecidos.	Rede	Proteger	●	●	●
	9.3	**Manter e impor filtros de URL baseados em rede** Imponha e atualize filtros de URL baseados em rede para limitar um ativo corporativo de se conectar a sites potencialmente maliciosos ou não aprovados. Exemplos de implementações incluem filtragem baseada em categoria, filtragem baseada em reputação ou através do uso de listas de bloqueio. Aplique filtros para todos os ativos corporativos.	Rede	Proteger		●	●
	9.4	**Restringir extensões de cliente de e-mail e navegador desnecessárias ou não autorizadas** Restrinja, seja desinstalando ou desabilitando, quaisquer plug-ins de cliente de e-mail ou navegador, extensões e aplicações complementares não autorizados ou desnecessários.	Aplicações	Proteger		●	●
	9.5	**Implementar o DMARC** Para diminuir a chance de e-mails forjados ou modificados de domínios válidos, implemente a política e verificação DMARC, começando com a implementação dos padrões Sender Policy Framework (SPF) e DomainKeys Identified Mail (DKIM).	Rede	Proteger		●	●
	9.6	**Bloquear tipos de arquivo desnecessários** Bloqueie tipos de arquivo desnecessários que tentem entrar no gateway de e-mail da empresa.	Rede	Proteger		●	●
	9.7	**Implantar e manter proteções antimalware de servidor de e-mail** Implante e mantenha proteção antimalware de servidores de e-mail, como varredura de anexos e/ou sandbox.	Rede	Proteger			●
10		**Defesas contra malware** Impedir ou controlar a instalação, disseminação e execução de aplicações, códigos ou scripts maliciosos em ativos corporativos.					
	10.1	**Instalar e manter um software anti-malware** Instale e mantenha um software anti-malware em todos os ativos corporativos.	Dispositivo	Proteger	●	●	●
	10.2	**Configurar atualizações automáticas de assinatura anti-malware** Configure atualizações automáticas para arquivos de assinatura anti-malware em todos os ativos corporativos.	Dispositivo	Proteger	●	●	●
	10.3	**Desabilitar a execução e reprodução automática para mídias removíveis** Desabilitar a funcionalidade de execução e reprodução automática para mídias removíveis.	Dispositivo	Proteger	●	●	●
	10.4	**Configurar a varredura anti-malware automática de mídia removivel** Configure o software anti-malware para verificar automaticamente a mídia removível.	Dispositivo	Detectar		●	●
	10.5	**Habilitar recursos anti-exploração** Habilite recursos anti-exploração em ativos e software corporativos, onde possível, como Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), ou Apple® System Integrity Protection (SIP) e Gatekeeper™.	Dispositivo	Proteger		●	●

CONTROLE	MEDIDAS DE SEGURANÇA	TÍTULO DA MEDIDA DE SEGURANÇA/ DESCRIÇÃO DA MEDIDA DE SEGURANÇA	TIPO DE ATIVO	FUNÇÃO DE SEGURANÇA	IG1	IG2	IG3
	10.6	**Gerenciar o software anti-malware de maneira centralizada** Gerencie o software anti-malware de maneira centralizada.	Dispositivo	Proteger		●	●
	10.7	**Usar software anti-malware baseado em comportamento** Use software anti-malware baseado em comportamento.	Dispositivo	Detectar		●	●
11		**Recuperação de dados** Estabeleça e mantenha práticas de recuperação de dados suficientes para restaurar ativos corporativos dentro do escopo para um estado pré-incidente e confiável.					
	11.1	**Estabelecer e manter um processo de recuperação de dados** Estabeleça e mantenha um processo de recuperação de dados. No processo, aborde o escopo das atividades de recuperação de dados, a priorização da recuperação e a segurança dos dados de backup. Revise e atualize a documentação anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.	Dados	Recuperar	●	●	●
	11.2	**Executar backups automatizados** Execute backups automatizados de ativos corporativos dentro do escopo. Execute backups semanalmente ou com mais frequência, com base na sensibilidade dos dados.	Dados	Recuperar	●	●	●
	11.3	**Proteger os dados de recuperação** Proteja os dados de recuperação com controles equivalentes dos dados originais. Referencie o uso de criptografia ou separação de dados, com base nos requisitos.	Dados	Proteger	●	●	●
	11.4	**Estabelecer e manter uma instância isolada de dados de recuperação** Estabeleça e mantenha uma instância isolada de dados de recuperação. Exemplos de implementações incluem controle de versão de destinos de backup por meio de sistemas ou serviços offline, na nuvem ou fora do site local.	Dados	Recuperar	●	●	●
	11.5	**Testar os dados de recuperação** Teste a recuperação do backup trimestralmente, ou com mais frequência, para uma amostra dos ativos corporativos dentro do escopo.	Dados	Recuperar		●	●
12		**Gestão da infraestrutura de rede** Estabeleça, implemente e gerencie ativamente (rastreie, reporte, corrija) os dispositivos de rede, a fim de evitar que atacantes explorem serviços de rede e pontos de acesso vulneráveis.					
	12.1	**Assegurar que a infraestrutura de rede esteja atualizada** Assegure que a infraestrutura de rede seja mantida atualizada. Exemplos de implementações incluem a execução da versão estável mais recente do software e/ou o uso de ofertas de network-as-a-service (NaaS) atualmente suportadas. Revise as versões do software mensalmente, ou com mais frequência, para verificar o suporte do software.	Rede	Proteger	●	●	●
	12.2	**Estabelecer e manter uma arquitetura de rede segura** Estabeleça e mantenha uma arquitetura de rede segura. Uma arquitetura de rede segura deve abordar segmentação, privilégio mínimo e disponibilidade, no mínimo.	Rede	Proteger		●	●
	12.3	**Gerenciar infraestrutura de rede com segurança** Gerencie com segurança a infraestrutura de rede. Exemplos de implementações incluem versão controlada de infraestrutura como código e o uso de protocolos de rede seguros, como SSH e HTTPS.	Rede	Proteger		●	●
	12.4	**Estabelecer e manter diagrama(s) de arquitetura** Estabeleça e mantenha diagrama(s) de arquitetura e/ou outra documentação de sistema de rede. Revise e atualize a documentação anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.	Rede	Identificar		●	●
	12.5	**Centralizar a autenticação, autorização e auditoria (AAA) de rede** Centralize AAA de rede.	Rede	Proteger		●	●

CONTROLE	MEDIDAS DE SEGURANÇA	TÍTULO DA MEDIDA DE SEGURANÇA/ DESCRIÇÃO DA MEDIDA DE SEGURANÇA	TIPO DE ATIVO	FUNÇÃO DE SEGURANÇA	IG1	IG2	IG3
	12.6	**Usar protocolos de comunicação e gestão de rede seguros** Use protocolos de comunicação e gestão de rede seguros (por exemplo, 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise ou superior).	Rede	Proteger		●	●
	12.7	**Assegurar que os dispositivos remotos utilizem uma VPN e estejam se conectando a uma infraestrutura AAA da empresa** Exigir que os usuários se autentiquem em serviços de autenticação e VPN gerenciados pela empresa antes de acessar os recursos da empresa em dispositivos de usuário final.	Dispositivo	Proteger		●	●
	12.8	**Estabelecer e manter recursos de computação dedicados para todo o trabalho administrativo** Estabeleça e mantenha recursos de computação dedicados, fisicamente ou logicamente separados, para todas as tarefas administrativas ou tarefas que requeiram acesso administrativo. Os recursos de computação devem ser segmentados da rede primária da empresa e não deve ser permitido o acesso à Internet.	Dispositivo	Proteger			●
13		**Monitoramento e defesa da Rede** Operar processos e ferramentas para estabelecer e manter monitoramento e defesa de rede abrangente contra ameaças de segurança em toda a infraestrutura de rede corporativa e base de usuários.					
	13.1	**Centralizar o alerta de eventos de segurança** Centralize os alertas de eventos de segurança em ativos corporativos para correlação e análise de log. A melhor prática requer o uso de um SIEM, que inclui alertas de correlação de eventos definidos pelo fornecedor. Uma plataforma de análise de log configurada com alertas de correlação relevantes para a segurança também atende a esta medida de segurança.	Rede	Detectar		●	●
	13.2	**Implantar solução de detecção de intrusão baseada em host** Implante uma solução de detecção de intrusão baseada em host em ativos corporativos, quando apropriado e/ou com suporte.	Dispositivo	Detectar		●	●
	13.3	**Implantar uma solução de detecção de intrusão de rede** Implante uma solução de detecção de intrusão de rede em ativos corporativos, quando apropriado. Exemplos de implementações incluem o uso de um Network Intrusion Detection System (NIDS) ou serviço de provedor de serviço de nuvem equivalente (CSP).	Rede	Detectar		●	●
	13.4	**Realizar filtragem de tráfego entre segmentos de rede** Execute a filtragem de tráfego entre segmentos de rede, quando apropriado.	Rede	Proteger		●	●
	13.5	**Gerenciar controle de acesso para ativos remotos** Gerencie o controle de acesso para ativos que se conectam remotamente aos recursos da empresa. Determine a quantidade de acesso aos recursos da empresa com base em: software anti-malware atualizado instalado, conformidade de configuração com o processo de configurações seguras da empresa e garantia de que o sistema operacional e as aplicações estão atualizados.	Dispositivo	Proteger		●	●
	13.6	**Coletar logs de fluxo de tráfego da rede** Colete logs de fluxo de tráfego de rede e/ou tráfego de rede para revisar e alertar sobre dispositivos de rede.	Rede	Detectar		●	●
	13.7	**Implantar solução de prevenção de intrusão baseada em host** Implante uma solução de prevenção de intrusão baseada em host em ativos corporativos, quando apropriado e/ou com suporte. Exemplos de implementações incluem o uso de um cliente Endpoint Detection and Response (EDR) ou agente IPS baseado em host.	Dispositivo	Proteger			●
	13.8	**Implantar uma solução de prevenção de intrusão de rede** Implante uma solução de prevenção de intrusão de rede, quando apropriado. Exemplos de implementações incluem o uso de um Network Intrusion Prevention System (NIPS) ou serviço CSP equivalente.	Rede	Proteger			●

CONTROLE	MEDIDAS DE SEGURANÇA	TÍTULO DA MEDIDA DE SEGURANÇA/ DESCRIÇÃO DA MEDIDA DE SEGURANÇA	TIPO DE ATIVO	FUNÇÃO DE SEGURANÇA	IG1	IG2	IG3
	13.9	**Implantar controle de acesso no nível de porta** Implante o controle de acesso no nível de porta. O controle de acesso no nível de porta utiliza 802.1x ou protocolos de controle de acesso à rede semelhantes, como certificados, e pode incorporar autenticação de usuário e/ou dispositivo.	Dispositivo	Proteger			●
	13.10	**Executar filtragem da camada de aplicação** Execute a filtragem da camada de aplicação. Exemplos de implementações incluem um proxy de filtragem, firewall de camada de aplicação ou gateway.	Rede	Proteger			●
	13.11	**Ajustar Limites de Alerta de Eventos de Segurança** Ajuste os limites de alerta de eventos de segurança mensalmente ou com mais frequência.	Rede	Detectar			●
14		**Conscientização sobre segurança e treinamento de competências** Estabelecer e manter um programa de conscientização de segurança para influenciar o comportamento da força de trabalho para ser consciente em segurança e devidamente qualificada para reduzir os riscos de segurança cibernética para a empresa.					
	14.1	**Estabelecer e manter um programa de conscientização de segurança** Estabeleça e mantenha um programa de conscientização de segurança. O objetivo de um programa de conscientização de segurança é educar a força de trabalho da empresa sobre como interagir com ativos e dados corporativos de maneira segura. Realize o treinamento na contratação e, no mínimo, anualmente. Revise e atualize o conteúdo anualmente ou quando ocorrerem mudanças significativas na empresa que possam afetar esta proteção.	N/A	Proteger	●	●	●
	14.2	**Treinar membros da força de trabalho para reconhecer ataques de engenharia social** Treine os membros da força de trabalho para reconhecer ataques de engenharia social, como phishing, pretexto e uso não autorizado.	N/A	Proteger	●	●	●
	14.3	**Treinar membros da força de trabalho nas melhores práticas de autenticação** Treine os membros da força de trabalho nas melhores práticas de autenticação. Exemplos de tópicos incluem MFA, composição de senha e gestão de credenciais	N/A	Proteger	●	●	●
	14.4	**Treinar a força de trabalho nas Melhores Práticas de Tratamento de Dados** Treine os membros da força de trabalho sobre como identificar, armazenar, transferir, arquivar e destruir dados sensíveis de maneira adequada. Isso também inclui o treinamento de membros da força de trabalho em práticas recomendadas de mesa e tela limpas, como bloquear a tela quando eles se afastam de seus ativos corporativos, apagar quadros brancos físicos e virtuais no final das reuniões e armazenar dados e ativos com segurança.	N/A	Proteger	●	●	●
	14.5	**Treinar membros da força de trabalho sobre as causas da exposição não intencional de dados** Treine os membros da força de trabalho para estarem cientes das causas da exposição não intencional de dados. Exemplos de tópicos incluem entrega incorreta de dados sensíveis, perda de um dispositivo de usuário final portátil ou publicação de dados para públicos indesejados.	N/A	Proteger	●	●	●
	14.6	**Treinar Membros da força de trabalho no Reconhecimento e Comunicação de Incidentes de Segurança** Treine os membros da força de trabalho para serem capazes de reconhecer um incidente em potencial e relatar tal incidente.	N/A	Proteger	●	●	●
	14.7	**Treinar a força de trabalho sobre como identificar e comunicar se o seus ativos corporativos estão faltando atualizações de segurança** Treine a força de trabalho para entender como verificar e relatar patches de software desatualizados ou quaisquer falhas em ferramentas e processos automatizados. Parte desse treinamento deve incluir a notificação do pessoal de TI sobre quaisquer falhas em processos e ferramentas automatizadas.	N/A	Proteger	●	●	●

CONTROLE	MEDIDAS DE SEGURANÇA	TÍTULO DA MEDIDA DE SEGURANÇA/ DESCRIÇÃO DA MEDIDA DE SEGURANÇA	TIPO DE ATIVO	FUNÇÃO DE SEGURANÇA	IG1	IG2	IG3
	14.8	**Treinar a força de trabalho sobre os perigos de se conectar e transmitir dados corporativos em redes inseguras** Treine os membros da força de trabalho sobre os perigos de se conectar e transmitir dados em redes inseguras para atividades corporativas. Se a empresa tiver funcionários remotos, o treinamento deve incluir orientação para garantir que todos os usuários configurem com segurança sua infraestrutura de rede doméstica.	N/A	Proteger	●	●	●
	14.9	**Conduzir treinamento de competências e conscientização de segurança para funções específicas** Conduza treinamento de conscientização de segurança e de competências específicas para funções. Exemplos de implementações incluem cursos de administração de sistema seguro para profissionais de TI, treinamento de conscientização e prevenção de vulnerabilidades para desenvolvedores de aplicações da web do OWASP® Top 10 aplicações e treinamento avançado de conscientização de engenharia social para funções de perfil alto.	N/A	Proteger		●	●
15		**Gestão de provedor de serviços** Desenvolva um processo para avaliar os provedores de serviços que mantêm dados sensíveis, ou são responsáveis por plataformas ou processos de TI críticos de uma empresa, para garantir que esses provedores estejam protegendo essas plataformas e dados de forma adequada.					
	15.1	**Estabelecer e manter um inventário de provedores de serviços** Estabeleça e mantenha um inventário de provedores de serviço. O inventário deve listar todos os provedores de serviços conhecidos, incluir classificação(ões) e designar um contato corporativo para cada provedor de serviços. Revise e atualize o inventário anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.	N/A	Identificar	●	●	●
	15.2	**Estabelecer e manter uma política de gestão de provedores de serviços** Estabeleça e mantenha uma política de gestão de provedores de serviços. Certifique-se de que a política trate da classificação, inventário, avaliação, monitoramento e descomissionamento de prestadores de serviços. Revise e atualize a política anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.	N/A	Identificar		●	●
	15.3	**Classificar provedores de serviços** Classifique os provedores de serviço. A consideração de classificação pode incluir uma ou mais características, como sensibilidade de dados, volume de dados, requisitos de disponibilidade, regulamentos aplicáveis, risco inerente e risco mitigado. Atualize e analise as classificações anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.	N/A	Identificar		●	●
	15.4	**Garantir que os contratos do provedor de serviços incluam requisitos de segurança** Certifique-se de que os contratos do provedor de serviços incluem requisitos de segurança. Requisitos de exemplo podem incluir requisitos mínimos do programa de segurança, notificação e resposta de incidente de segurança e/ou de violação de dados, requisitos de criptografia de dados e compromissos de descarte de dados. Esses requisitos de segurança devem ser consistentes com a política de gestão do provedor de serviços da empresa. Revise os contratos do provedor de serviços anualmente para garantir que os contratos não estejam perdendo os requisitos de segurança.	N/A	Proteger		●	●
	15.5	**Avaliar provedores de serviços** Avalie os provedores de serviços consistentes com a política de gestão de provedores de serviços da empresa. O escopo da avaliação pode variar com base na(s) classificação(ões) e pode incluir a revisão dos relatórios de avaliação padronizados, como Service Organization Control 2 (SOC 2) e Payment Card Industry (PCI) Attestation of Compliance (AoC), questionários personalizados ou outros processos rigorosos apropriados. Reavalie os prestadores de serviços anualmente, no mínimo, ou com contratos novos e renovados.	N/A	Identificar			●

CONTROLE	MEDIDAS DE SEGURANÇA	TÍTULO DA MEDIDA DE SEGURANÇA/ DESCRIÇÃO DA MEDIDA DE SEGURANÇA	TIPO DE ATIVO	FUNÇÃO DE SEGURANÇA	IG1	IG2	IG3
	15.6	**Monitorar provedores de serviços** Monitore os provedores de serviços de acordo com a política de gestão de provedores de serviços da empresa. O monitoramento pode incluir reavaliação periódica da conformidade do provedor de serviços, monitoramento dos release notes do provedor de serviços e monitoramento da dark web.	Dados	Detectar			●
	15.7	**Descomissionar com segurança os provedores de serviços** Descomissione os prestadores de serviços com segurança. Considerações de exemplo incluem desativação de contas de usuário e serviço, encerramento de fluxos de dados e descarte seguro de dados corporativos em sistemas de provedores de serviços.	Dados	Proteger			●
16		**Segurança de aplicações** Gerencie o ciclo de vida da segurança de software desenvolvido, hospedado ou adquirido internamente para prevenir, detectar e corrigir os pontos fracos de segurança antes que possam afetar a empresa.					
	16.1	**Estabelecer e manter um processo seguro de desenvolvimento de aplicações** Estabeleça e mantenha um processo seguro de desenvolvimento de aplicações. No processo, trate de itens como: padrões de design de aplicação seguro, práticas de codificação seguras, treinamento de desenvolvedor, gestão de vulnerabilidade, segurança de código de terceiros e procedimentos de teste de segurança de aplicação. Revise e atualize a documentação anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.	Aplicações	Proteger		●	●
	16.2	**Estabelecer e manter um processo para aceitar e endereçar vulnerabilidades de software** Estabelecer e manter um processo para aceitar e endereçar relatórios de vulnerabilidades de software, incluindo um meio para que as entidades externas relatem. O processo deve incluir itens como: uma política de tratamento de vulnerabilidade que identifica o processo de relatar, a parte responsável por lidar com os relatórios de vulnerabilidade e um processo de entrada, atribuição, correção e teste de correção. Como parte do processo, use um sistema de rastreamento de vulnerabilidade que inclua classificações de gravidade e métricas para medir o tempo de identificação, análise e correção de vulnerabilidades. Revise e atualize a documentação anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança. Os terceiros desenvolvedores de aplicações precisam considerar esta política para o exterior que ajuda a definir as expectativas para as partes interessadas externas.	Aplicações	Proteger		●	●
	16.3	**Executar análise de causa raiz em vulnerabilidades de segurança** Execute a análise de causa raiz em vulnerabilidades de segurança. Ao revisar as vulnerabilidades, a análise da causa raiz é a tarefa de avaliar os problemas subjacentes que criam vulnerabilidades no código e permite que as equipes de desenvolvimento vão além de apenas corrigir vulnerabilidades individuais conforme elas surgem.	Aplicações	Proteger		●	●
	16.4	**Estabelecer e gerenciar um inventário de componentes de software de terceiros** Estabeleça e gerencie um inventário atualizado de componentes de terceiros usados no desenvolvimento, geralmente chamados de "lista de materiais", bem como componentes programados para uso futuro. Este inventário deve incluir quaisquer riscos que cada componente de terceiros possa representar. Avalie a lista pelo menos uma vez por mês para identificar quaisquer mudanças ou atualizações nesses componentes e valide se o componente ainda é compatível.	Aplicações	Proteger		●	●
	16.5	**Usar componentes de software de terceiros atualizados e confiáveis** Use componentes de software de terceiros atualizados e confiáveis. Quando possível, escolha bibliotecas e estruturas estabelecidas e comprovadas que forneçam segurança adequada. Adquira esses componentes de fontes confiáveis ou avalie o software quanto a vulnerabilidades antes de usá-los.	Aplicações	Proteger		●	●

CONTROLE	MEDIDAS DE SEGURANÇA	TÍTULO DA MEDIDA DE SEGURANÇA/ DESCRIÇÃO DA MEDIDA DE SEGURANÇA	TIPO DE ATIVO	FUNÇÃO DE SEGURANÇA	IG1	IG2	IG3
	16.6	**Estabelecer e manter um sistema de classificação de gravidade e processo para vulnerabilidades de aplicações** Estabeleça e mantenha um sistema de classificação de gravidade e processo para vulnerabilidades de aplicações que facilitem a priorização da ordem em que as vulnerabilidades descobertas são corrigidas. Esse processo inclui a definição de um nível mínimo de aceitabilidade de segurança para a liberação de código ou aplicações. As classificações de gravidade trazem uma forma sistemática de triagem de vulnerabilidades que melhora o gestão de riscos e ajuda a garantir que os bugs mais graves sejam corrigidos primeiro. Revise e atualize o sistema e processo anualmente.	Aplicações	Proteger		●	●
	16.7	**Usar modelos de configurações de segurança padrão para infraestrutura de aplicações** Use modelos de configuração de segurança padrão recomendados pelo setor para componentes de infraestrutura de aplicações. Isso inclui servidores subjacentes, bancos de dados e servidores web e se aplica a contêineres de nuvem, componentes de Platform as a Service (PaaS) e componentes de SaaS. Não permita que o software desenvolvido internamente enfraqueça as configurações de segurança.	Aplicações	Proteger		●	●
	16.8	**Separar sistemas de produção e não produção** Mantenha ambientes separados para sistemas de produção e não produção.	Aplicações	Proteger		●	●
	16.9	**Treinar desenvolvedores em conceitos de segurança de aplicações e codificação segura** Certifique-se de que todo o pessoal de desenvolvimento de software receba treinamento para escrever código seguro para seu ambiente de desenvolvimento e responsabilidades específicas. O treinamento pode incluir princípios gerais de segurança e práticas padrão de segurança de aplicações. Conduza o treinamento pelo menos uma vez por ano e projete de forma a promover a segurança dentro da equipe de desenvolvimento e construir uma cultura de segurança entre os desenvolvedores.	Aplicações	Proteger		●	●
	16.10	**Aplicar princípios de design seguro em arquiteturas de aplicações** Aplique princípios de design seguro em arquiteturas de aplicações. Os princípios de design seguro incluem o conceito de privilégio mínimo e aplicação de mediação para validar cada operação que o usuário faz, promovendo o conceito de "nunca confiar nas entradas do usuário". Os exemplos incluem garantir que a verificação explícita de erros seja realizada e documentada para todas as entradas, incluindo tamanho, tipo de dados e intervalos ou formatos aceitáveis. O design seguro também significa minimizar a superfície de ataque da infraestrutura da aplicação, como desligar portas e serviços desprotegidos, remover programas e arquivos desnecessários e renomear ou remover contas padrão.	Aplicações	Proteger		●	●
	16.11	**Aproveitar os módulos ou serviços controlados para componentes de segurança de aplicações** Aproveite os módulos ou serviços controlados para os componentes de segurança da aplicação, como gestão de identidade, criptografia e auditoria e log. O uso de recursos da plataforma em funções críticas de segurança reduzirá a carga de trabalho dos desenvolvedores e minimizará a probabilidade de erros de design ou implementação. Os sistemas operacionais modernos fornecem mecanismos eficazes para identificação, autenticação e autorização e disponibilizam esses mecanismos para as aplicações. Use apenas algoritmos de criptografia padronizados, atualmente aceitos e amplamente revisados. Os sistemas operacionais também fornecem mecanismos para criar e manter logs de auditoria seguros.	Aplicações	Proteger		●	●
	16.12	**Implementar verificações de segurança em nível de código** Aplique ferramentas de análise estáticas e dinâmicas dentro do ciclo de vida da aplicação para verificar se as práticas de codificação seguras estão sendo seguidas.	Aplicações	Proteger			●

CONTROLE	MEDIDAS DE SEGURANÇA	TÍTULO DA MEDIDA DE SEGURANÇA/ DESCRIÇÃO DA MEDIDA DE SEGURANÇA	TIPO DE ATIVO	FUNÇÃO DE SEGURANÇA	IG1	IG2	IG3
	16.13	**Realizar teste de invasão de aplicação** Realize teste de invasão das aplicações. Para aplicações críticas, o teste de invasão autenticado é mais adequado para localizar vulnerabilidades de lógica de negócios do que a varredura de código e o teste de segurança automatizado. O teste de invasão depende da habilidade do testador para manipular manualmente um aplicação como um usuário autenticado e não autenticado.	Aplicações	Proteger			●
	16.14	**Conduzir aplicações de modelagem de ameaças** Conduza a modelagem de ameaças. A modelagem de ameaças é o processo de identificar e abordar as falhas de design de segurança da aplicação em um design, antes que o código seja criado. É conduzido por pessoas especialmente treinadas que avaliam o design da aplicação e medem os riscos de segurança para cada ponto de entrada e nível de acesso. O objetivo é mapear a aplicação, a arquitetura e a infraestrutura de uma forma estruturada para entender seus pontos fracos.	Aplicações	Proteger			●
17		**Gestão de respostas a incidentes** Estabelecer um programa 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.					
	17.1	**Designar Pessoal para Gerenciar Tratamento de Incidentes** Designe uma pessoa-chave e pelo menos uma backup para gerenciar o processo de tratamento de incidentes da empresa. A equipe de gestão é responsável pela coordenação e documentação dos esforços de resposta e recuperação a incidentes e pode consistir em funcionários internos da empresa, fornecedores terceirizados ou uma abordagem híbrida. Se estiver usando um fornecedor terceirizado, designe pelo menos uma pessoa interna da empresa para supervisionar qualquer trabalho terceirizado. Revise anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.	N/A	Responder	●	●	●
	17.2	**Estabelecer e manter informações de contato para relatar incidentes de segurança** Estabeleça e mantenha as informações de contato das partes que precisam ser informadas sobre os incidentes de segurança. Os contatos podem incluir funcionários internos, fornecedores terceirizados, policiais, provedores de seguros cibernéticos, agências governamentais relevantes, parceiros do Information Sharing and Analysis Center (ISAC) ou outras partes interessadas. Verifique os contatos anualmente para garantir que as informações estejam atualizadas.	N/A	Responder	●	●	●
	17.3	**Estabelecer e manter um processo corporativo para relatar incidentes** Estabeleça e mantenha um processo corporativo para a força de trabalho relatar incidentes de segurança. O processo inclui cronograma de relatórios, pessoal para relatar, mecanismo para relatar e as informações mínimas a serem relatadas. Certifique-se de que o processo esteja publicamente disponível para toda a força de trabalho. Revise anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.	N/A	Responder	●	●	●
	17.4	**Estabelecer e manter um processo de resposta a incidentes** Estabeleça e mantenha um processo de resposta a incidentes que aborde funções e responsabilidades, requisitos de conformidade e um plano de comunicação. Revise anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.	N/A	Responder		●	●
	17.5	**Atribuir funções e responsabilidades chave** Atribua funções e responsabilidades chave para resposta a incidentes, incluindo equipe jurídica, TI, segurança da informação, instalações, relações públicas, recursos humanos, respondentes a incidentes e analistas, conforme aplicável. Revise anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.	N/A	Responder		●	●
	17.6	**Definir mecanismos de comunicação durante a resposta a incidente** Determine quais mecanismos primários e secundários serão usados para se comunicar e relatar durante um incidente de segurança. Os mecanismos podem incluir ligações, e-mails ou cartas. Lembre-se de que certos mecanismos, como e-mails, podem ser afetados durante um incidente de segurança. Revise anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.	N/A	Responder		●	●

CONTROLE	MEDIDAS DE SEGURANÇA	TÍTULO DA MEDIDA DE SEGURANÇA/ DESCRIÇÃO DA MEDIDA DE SEGURANÇA	TIPO DE ATIVO	FUNÇÃO DE SEGURANÇA	IG1	IG2	IG3
	17.7	**Conduzir exercícios de resposta a incidentes rotineiros** Planeje e conduza exercícios de resposta a incidentes rotineiros e cenários para o pessoal-chave envolvido no processo de resposta a incidentes para se preparar para responder a incidentes do mundo real. Os exercícios precisam testar os canais de comunicação, tomada de decisão e fluxos de trabalho. Realize testes anualmente, no mínimo.	N/A	Recuperar		●	●
	17.8	**Conduzir análises pós-incidente** Realize análises pós-incidente. As análises pós-incidente ajudam a prevenir a recorrência do incidente por meio da identificação de lições aprendidas e ações de acompanhamento.	N/A	Recuperar		●	●
	17.9	**Estabelecer e manter limites de incidentes de segurança** Estabeleça e mantenha limites de incidentes de segurança, incluindo, no mínimo, a diferenciação entre um incidente e um evento. Os exemplos podem incluir: atividade anormal, vulnerabilidade de segurança, fraqueza de segurança, violação de dados, incidente de privacidade, etc. Revise anualmente ou quando ocorrerem mudanças corporativas significativas que possam impactar esta medida de segurança.	N/A	Recuperar			●
18		**Testes de invasão** Teste a eficácia e a resiliência dos ativos corporativos por meio da identificação e exploração de fraquezas nos controles (pessoas, processos e tecnologia) e da simulação dos objetivos e ações de um atacante.					
	18.1	**Estabelecer e manter um programa de teste de invasão** Estabeleça e mantenha um programa de teste de invasão adequado ao tamanho, complexidade e maturidade da empresa. As características do programa de teste de invasão incluem escopo, como rede, aplicação web, Application Programming Interface (API), serviços hospedados e controles de instalações físicas; frequência; limitações, como horas aceitáveis e tipos de ataque excluídos; informações do ponto de contato; remediação, por exemplo, como as descobertas serão encaminhadas internamente; e requisitos retrospectivos.	N/A	Identificar		●	●
	18.2	**Realizar testes de invasão externos periódicos** Realize testes de invasão externos periódicos com base nos requisitos do programa, pelo menos uma vez por ano. O teste de invasão externo deve incluir reconhecimento empresarial e ambiental para detectar informações exploráveis. O teste de invasão requer habilidades e experiência especializadas e deve ser conduzido por uma parte qualificada. O teste pode ser clear box ou opaque box.	Rede	Identificar		●	●
	18.3	**Corrigir as descobertas do teste de invasão** Corrija as descobertas do teste de invasão com base na política da empresa para o escopo e a priorização da correção.	Rede	Proteger		●	●
	18.4	**Validar as Medidas de Segurança** Valide as medidas de segurança após cada teste de invasão. Se necessário, modifique os conjuntos de regras e recursos para detectar as técnicas usadas durante o teste.	Rede	Proteger			●
	18.5	**Realizar testes de invasão internos periódicos** Realize testes de invasão internos periódicos com base nos requisitos do programa, pelo menos uma vez por ano. O teste pode ser clear box ou opaque box.	N/A	Identificar			●

CIS Center for Internet Security®

CIS Controls

The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation. We are a community-driven nonprofit, responsible for the CIS Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats.

Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud. CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the rapidly changing cybersecurity needs of U.S. elections offices. To learn more, visit www.cisecurity.org or follow us on Twitter: @CISecurity.

cisecurity.org
info@cisecurity.org
518-266-3460
Center for Internet Security
@CISecurity
CenterforIntSec
TheCISecurity
cisecurity