

Guia do Framework de Segurança

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

Versão2.0

Brasília, janeiro de 2022

GUIA DO FRAMEWORK DE SEGURANÇA

Lei Geral de Proteção de Dados Pessoais

MINISTÉRIO DA ECONOMIA

Paulo Roberto Nunes Guedes

Ministro

SECRETARIA ESPECIAL DE DESBUROCRATIZAÇÃO, GESTÃO E GOVERNO DIGITAL

Caio Mário Paes de Andrade

Secretário Especial de Desburocratização, Gestão e Governo Digital

SECRETARIA DE GOVERNO DIGITAL

Fernando André Coelho Mitkiewicz

Secretário de Governo Digital

DEPARTAMENTO DE GOVERNANÇA DE DADOS E INFORMAÇÕES

Leonardo Rodrigo Ferreira

Diretor do Departamento de Governança de Dados e Informações

COORDENAÇÃO-GERAL DE SEGURANÇA DA INFORMAÇÃO

Loriza Andrade Vaz de Melo

Coordenadora-Geral de Segurança da Informação

EQUIPE TÉCNICA DE ELABORAÇÃO

Denis Marcelo Oliveira

Julierme Rodrigues da Silva

Luiz Henrique do Espírito Santo Andrade

Tássio Correia da Silva

Wellington Francisco Pinheiro de Araújo

EQUIPE TÉCNICA DE ATUALIZAÇÃO

Álvaro Sergio de Souza Junior

Amaury C. da Silveira Junior

Bruno Pierre Rodrigues de Sousa
Éder Ferreira de Andrade
Francisco Magno Felix Nobre
Heráclito Ricardo Ferreira Gomes
Francisco Magno Felix Nobre
Ivaldo Jeferson de Santana Castro
Raphael César Estevão
Yuri Arcanjo de Carvalho

EQUIPE REVISORA

Marcelo de Lima
Marcus Paulo Barbosa Vasconcelos
Samuel Barichello Conceição

Histórico de Versões

Data	Versão	Descrição	Autor
12/04/2021	1.0	Primeira versão do Guia do Framework de Segurança.	Equipe Técnica de Elaboração
15/12/2021	2.0	Segunda versão do Guia do Framework de Segurança, atualização dos controles com base no CIS versão 8.	Equipe Técnica de Atualização

SUMÁRIO

AVISO PRELIMINAR E AGRADECIMENTOS	6
INTRODUÇÃO.....	8
1 - CIS.....	9
2 – NIST	12
3 - Controles do CIS	14
CIS Controle 1: Inventário e Controle de Ativos Institucionais	14
CIS Controle 2: Inventário e Controle de Ativos de Software	16
CIS Controle 3: Proteção de Dados	17
CIS Controle 4: Configuração Segura de Ativos Institucionais e Software	19
CIS Controle 5: Gestão de Contas	21
CIS Controle 6: Gestão do Controle de Acesso	22
CIS Controle 7: Gestão Contínua de Vulnerabilidades	23
CIS Controle 8: Gestão de Registros de Auditoria	25
CIS Controle 9: Proteções de E-mail e Navegador Web.....	27
CIS Controle 10: Defesas Contra Malware	28
CIS Controle 11: Recuperação de Dados.....	29
CIS Controle 12: Gestão da Infraestrutura de Rede.....	30
CIS Controle 13: Monitoramento e Defesa da Rede	32
CIS Controle 14: Conscientização e Treinamento de Competências sobre Segurança	33
CIS Controle 15: Gestão de Provedor de Serviços	35
CIS Controle 16: Segurança de Aplicações.....	37
CIS Controle 17: Gestão de Resposta a Incidentes	40
CIS Controle 18: Testes de Invasão	43
4 - Ferramenta de Acompanhamento da Implementação dos Controles do CIS	44
4.1 Estrutura e Organização da Ferramenta.....	45
4.2 Níveis de Maturidade e demais Cálculos.....	47
4.3 Gráfico do Dashboard ATT&CK Activity	51
ANEXO I	61
ANEXO II Mudanças desta versão.....	68

AVISO PRELIMINAR E AGRADECIMENTOS

O presente guia busca compartilhar e difundir as melhores práticas internacionais em matéria de segurança da informação, algumas das quais não se encontram integralmente disponíveis em língua portuguesa. O documento é especialmente recomendado e dirigido aos órgãos e às entidades da Administração Pública Federal brasileira para auxiliar o atendimento do capítulo VII “Da segurança e das boas práticas” da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709, de 14 de agosto de 2018), mas poderá também ser aproveitado por outras instituições que busquem informações sobre o tema.

O guia é de autoria exclusiva da Secretaria de Governo Digital do Ministério da Economia, mas contém referências a publicações e a outros documentos técnicos, com destaque para aqueles do Center for Internet Security (CIS)¹, do AuditScripts² e do National Institute of Standards and Technology (NIST)³. Muitas das referências foram traduzidas de forma livre pelos técnicos do governo brasileiro, com propósitos educativos e não comerciais e com o objetivo de democratizar e de ampliar o acesso a tais conhecimentos no país.

Ao proceder desse modo, a Secretaria de Governo Digital enfatiza que: a) não representa, tampouco se manifesta em nome do CIS, do AuditScripts e do NIST, e vice-versa; b) não é coautora das publicações internacionais abordadas; c) não assume nenhuma responsabilidade administrativa, técnica ou jurídica pelo uso ou pela interpretação inadequados, fragmentados ou parciais do presente guia; e d) caso o leitor deseje se certificar de que atende integralmente os requisitos das publicações do CIS, do AuditScripts e do NIST em suas versões originais, na língua inglesa, deverá consultar diretamente as fontes oficiais de informação ofertadas pelas referidas instituições.

Um agradecimento especial deve ser registrado ao CIS, ao AuditScripts e ao NIST pelas valiosas contribuições para a comunidade de segurança da informação,

¹ Disponível em <https://www.cisecurity.org/>

² Disponível em <https://www.auditscripts.com/>

³ Disponível em <https://www.nist.gov/cyberframework/framework>

bem como ao Gabinete de Segurança Institucional da Presidência da República (GSI/PR), ao SERPRO e a DATAPREV pelas contribuições na revisão deste Guia.

INTRODUÇÃO

O guia do Framework de Segurança é uma adição à série de guias operacionais⁴ elaborados pela Secretaria de Governo Digital (SGD), da Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia para fomentar a adequação à proteção dos dados pessoais^{5,6,7}. O Guia de Avaliação de Riscos de Segurança e Privacidade⁸, é de especial relevância e poderá ser utilizado diretamente como complemento deste, visto que, à medida que os controles são implementados, pode-se avaliar um determinado sistema crítico diante dos riscos aos dados pessoais tratados⁹. A avaliação descrita no Guia de Avaliação de Riscos de Segurança e Privacidade é realizada por uma ferramenta de acesso aberto ao público¹⁰.

O objetivo deste Guia do Framework de Segurança é fornecer aos profissionais de segurança da informação uma maneira de iniciar a identificação, o acompanhamento e o preenchimento das lacunas de segurança da informação presentes na instituição em relação aos 18 Controles de Segurança elaborados pelo CIS.

Para tanto, o Guia é inspirado nos documentos: CIS Control, versão 8, CIS Critical Security Control v8.0 Assessment Tool e Framework for Improving Critical Infrastructure Cybersecurity, versão 1.1. O Guia não substitui a leitura dos documentos originais na busca por informações complementares.

⁴ Disponível em <https://www.gov.br/governodigital/pt-br/governanca-de-dados/guias-operacionais-para-adequacao-a-lgpd>

⁵ Decreto nº 9.745, de 8 de abril de 2019. Art. 132, IV - apoiar ações de fomento a segurança da informação e proteção a dados pessoais no âmbito da administração pública federal, em articulação com os órgãos responsáveis por essas políticas.

⁶ Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em 28 fev. 2021.

⁷ Guia de Boas Práticas LGPD. Disponível em: <https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-de-boas-praticas-lei-geral-de-protecao-de-dados-lgpd>. Acesso em 28 fev. 2021.

⁸ Disponível em: <https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-de-avaliacao-de-riscos-de-seguranca-e-privacidade.pdf>

⁹ Lei nº 13.709/2018, art. 5º, inciso X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. 10

¹⁰ Disponível em <https://pesquisa.sisp.gov.br/index.php/468289?lang=pt-BR>

Ao longo do Guia, são abordados os Grupos de Implementação do CIS, as Funções da Estrutura Básica do Guia de Aperfeiçoamento da Segurança Cibernética para Infraestrutura Crítica do NIST e os 18 Controles do CIS.

A Ferramenta de Acompanhamento da Implementação dos Controles do CIS oferece a possibilidade de acompanhar a implementação dos 18 controles do CIS por meio da alimentação de informações numa planilha com gráficos que permitem identificar o estágio atual da instituição. Essa ferramenta é complementar a este Guia e sofreu adaptações, a fim de manter integração aos projetos desenvolvidos pelas equipes técnicas da Secretaria de Governo Digital. O Capítulo 4 descreve o seu funcionamento.

Esse documento é uma atualização da versão 1.0. Deste modo, a SGD apresenta no anexo II as mudanças e justificativas com relação a publicação anterior.

O Guia será atualizado à medida que novos ajustes forem necessários para acompanhar o amadurecimento dos processos de segurança da informação.

Ressalta-se que a instituição é livre para adequar todas as proposições deste guia a sua realidade. A abordagem proposta por este registro oferece uma orientação generalizada para priorizar o uso dos Controles do CIS, mas esse fato não exclui a necessidade de que a instituição compreenda sua própria postura de risco institucional. A intenção é ajudar a organização a concentrar seus esforços com base nos recursos disponíveis, integrando-os a qualquer processo de gestão de risco pré-existente.

No mesmo sentido, deve ser ressaltado que a adoção do presente guia não equivale necessariamente a cumprir a legislação brasileira sobre segurança, privacidade e proteção de dados pessoais, em especial a Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD). Contudo, o presente documento seguramente poderá auxiliar a instituição adotante a atingir os objetivos previstos nas normas correlatas, ao permitir a visualização da maturidade de seus trabalhos de segurança da informação e de proteção de dados e ampliar a implementação das melhores práticas sobre o tema.

1 - CIS

Os Controles do CIS (Center for Internet Security, Inc.) são um conjunto de ações priorizadas que atuam coletivamente na defesa de sistemas e infraestrutura por meio das melhores práticas para mitigar os mais comuns tipos de ataques. Os controles foram desenvolvidos por profissionais experientes e dos mais diversos setores da economia incluindo saúde, manufatura, educação, governo, defesa e outros.

As medidas contidas nos controles do CIS auxiliam a detecção, a resposta e a mitigação de danos dos mais comuns aos mais avançados tipos de ataque. Dessa forma, há medidas com mais complexidade em serem estabelecidas que outras. Entretanto, para atender os mais variados tipos de instituições, foram criados três Grupos de Implementação (GI). Cada um indica medidas de segurança específicas que devem ser atendidas e são cumulativas a cada grupo avançado. Logo, o Grupo de Implementação 2, abrange o Grupo de Implementação 1, ao passo que o Grupo de Implementação 3, abrange os Grupos de Implementação 1 e 2, conforme exemplifica a Figura 1.

Grupo de Implementação 1:

É representado por uma instituição de pequeno a médio porte com limitado corpo de profissionais de TI e experiência em cibersegurança. A sensibilidade dos dados a serem protegidos é baixa e envolve principalmente informações financeiras e de funcionários. A principal preocupação de instituições com essas características é manter o negócio operacional, pois elas têm uma tolerância limitada para o tempo de inatividade. Caso haja dados mais sensíveis, como por exemplo dados de cidadãos obtidos ou armazenados devido a alguma prestação de serviço público, a instituição deve atender as medidas do grupo de implementação superior (mais elevado). As medidas de segurança selecionadas para o Grupo de Implementação 1 podem ser implementadas por equipes de TI com experiência limitada em segurança cibernética e essas medidas são destinadas a impedir ataques gerais não direcionados.

Grupo de Implementação 2:

É representado por uma instituição com profissionais dedicados a gerenciar e proteger a infraestrutura de TI. A instituição que se encontra no Grupo de Implementação 2 geralmente armazena e processa informações confidenciais/sensíveis de cidadãos¹¹, o que inclui dados pessoais¹², e pode resistir a curtas interrupções de serviço. Uma evidente preocupação é a perda de confiança do cidadão se ocorrer uma violação aos seus dados. As medidas de segurança selecionadas para o Grupo de Implementação 2 ajudam as equipes de segurança a lidar com o aumento da complexidade operacional. Algumas medidas de segurança dependerão de tecnologia de nível empresarial e conhecimento especializado para instalar e configurar adequadamente.

Grupo de Implementação 3:

É representado por uma instituição que emprega **especialistas em segurança** capacitados em diferentes aspectos da segurança cibernética, tais como, gerenciamento de risco, teste de penetração e segurança de aplicativo. Uma instituição do Grupo de Implementação 3 deve abordar a disponibilidade de serviços e a confidencialidade e integridade dos dados sensíveis. Ataques bem-sucedidos à instituição podem causar danos significativos ao bem-estar público. As medidas de segurança selecionadas para o Grupo de Implementação 3 devem diminuir os ataques direcionados de um adversário sofisticado e reduzir o impacto dos ataques zero-day.

Reforça-se que os três grupos acima referidos tentam criar uma identificação de perfil e ajudar a instituição no amadurecimento das linhas de defesa, de forma gradativa. Esse quadro não impede que medidas de segurança de perfil mais avançado sejam implementados na instituição. A figura abaixo resume a visão dos grupos de implementação:

¹¹ Lei nº 13.709/2018, art. 5º, inciso II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

¹² Lei nº 13.709/2018, art. 5º, inciso I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável.

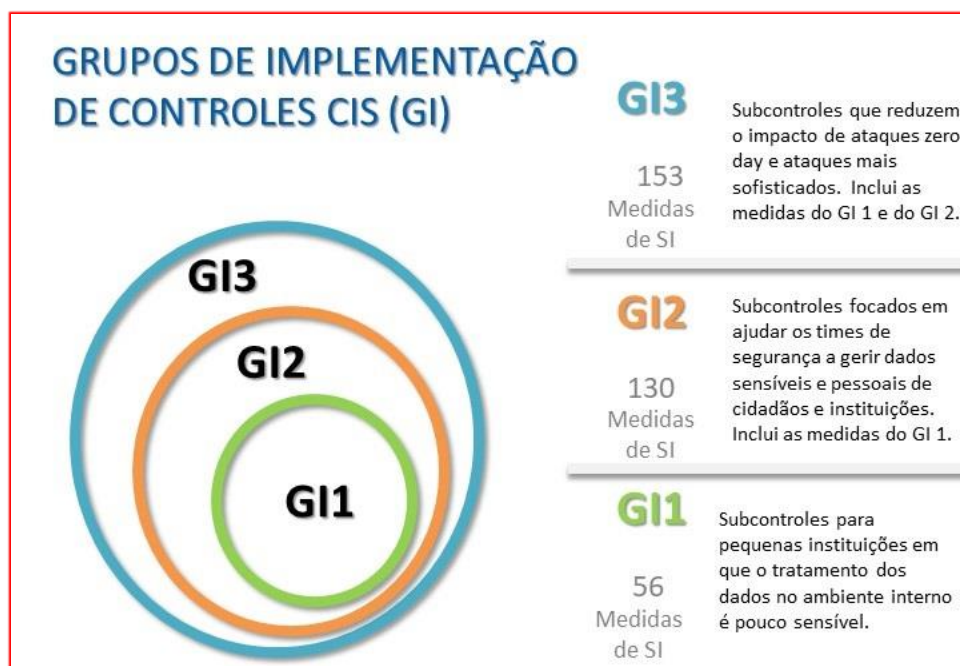


Figura 1. Adaptado do CIS Control v8

2 – NIST

O CIS dentro das suas medidas de segurança enquadra as cinco funções de Segurança da Estrutura Básica definidas na publicação **Guia de Aperfeiçoamento da Segurança Cibernética para Infraestrutura Crítica**¹³ do NIST. As cinco funções são: identificar, proteger, detectar, responder e recuperar.

Para este documento, um dos objetivos da inclusão das cinco funções é facilitar a classificação das ações (implementação das medidas de segurança) em um plano de tratamento de riscos. Caso os planos já existam, recomenda-se que os gestores possam dar continuidade a essa proposição e adequem as medidas de segurança às ações dos seus planos de tratamento de riscos.

Abaixo estão as definições de Estrutura Básica das funções presentes no NIST:

¹³ Disponível em https://www.uschamber.com/sites/default/files/intl_nist_framework_portuguese_finalfull_web.pdf

A Estrutura Básica é um conjunto de atividades de segurança cibernética, resultados desejados e referências aplicáveis que são comuns em setores de infraestrutura crítica. A Estrutura Básica apresenta padrões, diretrizes e práticas da indústria de maneira a permitir a comunicação das atividades e dos resultados da segurança cibernética em toda a organização, desde o nível executivo até o nível de implementação ou operacional.

A Estrutura Básica consiste de cinco funções simultâneas e contínuas — **Identificar, Proteger, Detectar, Responder e Recuperar**. Quando analisadas em conjunto, essas funções fornecem uma visão estratégica de alto nível do ciclo de vida do gerenciamento do risco de segurança cibernética de uma organização.

Identificar - Desenvolver uma compreensão organizacional para gerenciar o risco de segurança cibernética no que tange a sistemas, pessoas, ativos, dados e recursos.

- As atividades na **Função Identificar** são fundamentais para o uso eficiente do Guia de Aperfeiçoamento da Segurança Cibernética para Infraestrutura Crítica. Uma organização é capaz de focar e priorizar seus esforços de forma consistente com sua estratégia de gerenciamento de riscos e demandas empresariais, a partir da compreensão do contexto de seu nicho, dos recursos que suportam funções críticas e dos riscos de segurança cibernética envolvidos. Os exemplos de Categorias de resultados dentro desta Função incluem: Gerenciamento de Ativos; Ambiente Empresarial; Governança; Avaliação de Risco; e Estratégia de Gerenciamento de Risco.

Proteger - Desenvolver e implementar proteções necessárias para garantir a prestação de serviços críticos.

- A **Função Proteger** fornece apoio à capacidade de limitar ou conter o impacto de uma possível ocorrência de segurança cibernética. Os exemplos de Categorias de resultados dentro desta Função incluem: Gerenciamento de Identidade e Controle de Acesso; Conscientização e Treinamento; Segurança de Dados; Processos e Procedimentos de Proteção da Informação; Manutenção; e Tecnologia de Proteção.

Detectar - Desenvolver e implementar atividades necessárias para identificar a ocorrência de um evento de segurança cibernética.

- A **Função Detectar** permite a descoberta oportuna de ocorrências de segurança cibernética. Os exemplos de Categorias de resultados dentro desta Função incluem: Anomalias e Ocorrências; Monitoramento Contínuo

de Segurança; e Processos de Detecção.

Responder - Desenvolver e implementar atividades apropriadas para agir contra um incidente de segurança cibernética detectado.

- A **Função Responder** suporta a capacidade de conter o impacto de um possível incidente de segurança cibernética. Exemplos de Categorias de resultados dentro desta Função incluem: Planejamento de Resposta; Notificações; Análise; Mitigação; e Aperfeiçoamentos.

Recuperar - Desenvolver e implementar atividades apropriadas para manter planos de resiliência e restaurar quaisquer recursos ou serviços que foram prejudicados devido a um incidente de segurança cibernética.

- A **Função Recuperar** oferece apoio ao restabelecimento pontual para as operações normais de modo a reduzir o impacto de determinado incidente de segurança cibernética. Os exemplos de Categorias de resultados dentro desta Função incluem: Planejamento de Restabelecimento; Aperfeiçoamentos; e Notificações.

3 - Controles do CIS

Este capítulo expõe cada um dos 18 controles do CIS, suas respectivas medidas de segurança e a indicação do grupo de implementação correlato.

CIS Controle 1: Inventário e Controle de Ativos Institucionais

Gerencie ativamente (inventarie, rastreie e corrija) todos os dispositivos de hardware na rede para que apenas os dispositivos autorizados tenham acesso e os dispositivos não autorizados e não gerenciados sejam encontrados e impedidos de obter acesso.

Por que implementar?

Da mesma forma que se você não pode medir, não pode gerenciar, as

organizações não conseguem defender-se do que não sabem que possuem. O Inventário e controle de ativos institucionais desempenha um papel crítico no monitoramento de segurança, resposta a incidentes, backup e recuperação de sistemas. As organizações devem saber quais dados são essenciais para elas, e a gestão adequada de ativos ajudará a identificar os ativos institucionais que mantêm ou gerenciam esses dados críticos, para que as medidas de segurança apropriadas possam ser aplicadas. Isso também ajudará na identificação de ativos não autorizados e não gerenciados para removê-los ou remediá-los.

Vale ressaltar que entram na lista de ativos:

- dispositivos de usuário final (computador institucional, dispositivos portáteis e móveis);
- dispositivos de rede;
- dispositivos não computacionais;
- Internet das Coisas (IoT);
- Servidores (conectados fisicamente à infraestrutura, virtualmente, remotamente, e aqueles em ambientes de nuvem)

CIS Controle 1: Inventário e Controle de Ativos Institucionais

ID	NIST CSF	Medida de Segurança	Descrição da Medida de Segurança	Grupo de Implementação
1.1	Identificar	Estabelecer e manter um inventário detalhado de ativos institucionais	Estabelecer e manter um inventário preciso, detalhado e atualizado de todos os ativos institucionais com potencial para armazenar ou processar dado. Certificar de que o inventário registrará o endereço de rede (se estático), endereço de hardware, nome da máquina, etc. Deverá incluir ativos conectados à infraestrutura física, virtual, e remota e aqueles dentro de ambientes de nuvem. Necessário incluir também ativos mesmo que não estejam sob controle do órgão. Revisar e atualizar o inventário semestralmente ou com mais frequência	1 2 3
1.2	Responder	Endereçar ativos não autorizados	Assegurar que exista um processo semanal para lidar com ativos não autorizados. Optar por remover o ativo da rede, negar que o ativo se conecte remotamente à rede ou colocar o ativo em quarentena.	1 2 3
1.3	Detectar	Usar uma ferramenta de descoberta ativa	Identificar ativos conectados à rede institucional através de uma ferramenta de descoberta ativa. Configurar para que essa descoberta seja executada diariamente ou com mais frequência.	2 3
1.4	Identificar	Usar o <i>Dynamic Host Configuration Protocol</i> (DHCP) para Atualizar o Inventários de Ativos	Utilizar o registro (logs) do <i>Dynamic Host Configuration Protocol</i> (DHCP) em todos os servidores DHCP ou utilizar uma ferramenta de gerenciamento de endereços IP para atualizar o inventário de ativos de hardware da instituição.	2 3

1.5	Detectar	Ferramenta de Descoberta Passiva	Utilizar uma ferramenta de descoberta passiva para identificar dispositivos conectados à rede da instituição e automaticamente atualizar o inventário de ativos de hardware da instituição.	3
-----	----------	----------------------------------	---	---

CIS Controle 2: Inventário e Controle de Ativos de Software

Gerencie ativamente (inventarie, rastreie e corrija) todo o software na rede para que apenas o software autorizado seja instalado e possa ser executado, e que todo o software não autorizado e não gerenciado seja encontrado e impedido de instalação ou execução.

Por que implementar?

Um inventário de software completo é um recurso crítico para prevenir ataques. Os atacantes realizam varreduras na infraestrutura do órgão continuamente em busca de versões vulneráveis de software que possam ser exploradas. Contudo, sem um inventário completo dos ativos de software, um órgão não pode determinar se possui software vulnerável ou se há violações de licenciamento em potencial.

É fundamental inventariar, compreender, avaliar e gerenciar todos os softwares conectados à infraestrutura. Além de revisar seu inventário de software para identificar quaisquer ativos executando software que não sejam necessários para suas atividades.

CIS Controle 2: Inventário e Controle de Ativos de Software

ID	NIST CSF	Medida de Segurança	Descrição da Medida de Segurança	Grupo de Implementação
2.1	Identificar	Estabelecer e manter um inventário de software	Estabelecer e manter um inventário detalhado de todos os softwares licenciados instalados em ativos. Revisar e atualizar o inventário de software semestralmente ou com mais frequência.	1 2 3
2.2	Identificar	Assegurar que o software autorizado seja atualmente suportado	Garantir que apenas aplicações ou sistemas operacionais atualmente suportados pelo fabricante sejam adicionados ao inventário de softwares autorizados. Softwares não suportados devem ser indicados no sistema de inventário. Revisar o inventário de software para verificar o suporte do software pelo menos uma vez por mês ou com mais frequência.	1 2 3
2.3	Responder	Endereçar o software não autorizado	Assegurar que o software não autorizado seja retirado de uso em ativos institucionais ou receba uma exceção documentada. Revisar mensalmente ou com mais frequência.	1 2 3

2.4	Detectar	Utilizar ferramentas automatizadas de inventário de software	Utilizar ferramentas de inventário de software, quando possível, em toda a organização para automatizar a descoberta e documentação do software instalado.	2 3
2.5	Proteger	Lista de permissões de Software autorizado	Utilizar controles técnicos em todos os ativos para garantir que apenas software autorizado seja executado. Reavaliar semestralmente ou com mais frequência.	2 3
2.6	Proteger	Lista de permissões de bibliotecas autorizadas	Utilizar controles técnicos para garantir que apenas bibliotecas autorizadas (tais como *.dll, *.ocx, *.so, etc) tenham permissão para serem carregadas nos processos em execução. Impedir que bibliotecas não autorizadas sejam carregadas nos processos. Reavaliar semestralmente ou com mais frequência.	2 3
2.7	Proteger	Lista de permissões de Scripts autorizados	Utilize controles técnicos como assinaturas digitais e controle de versão para garantir que apenas scripts autorizados e assinados digitalmente (tais como *.ps1, *.py, macros etc.) tenham permissão para serem executados. Bloqueie a execução de scripts não autorizados. Reavalie semestralmente ou com mais frequência.	3

CIS Controle 3: Proteção de Dados

Utilize processos e ferramentas para evitar e mitigar a violação de dados, e garantir a privacidade e integridade das informações sensíveis e pessoais.

Por que implementar?

No momento atual sabemos que os dados não estão mais apenas dentro da estrutura das instituições; podemos ter dados na nuvem, em dispositivos portáteis do usuário final, compartilhados com parceiros ou serviços online em qualquer lugar do mundo.

As organizações possuem uma série de dados, que são importantes para o negócio, dentre eles os dados pessoais. O tratamento desses dados deve estar de acordo com a LGPD e demais regulamentações de proteção de dados e privacidade pois a não conformidade pode acarretar em prejuízos financeiros e reputacionais.

A privacidade de dados tornou-se cada vez mais importante e as organizações 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.

A perda de controle da organização sobre os dados protegidos ou sensíveis é um sério e frequentemente relatado impacto no negócio. 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.

CIS Controle 3: Proteção de Dados

ID	NIST CSF	Medida de Segurança	Descrição da Medida de Segurança	Grupo de Implementação
3.1	Identificar	Estabelecer e manter um processo de gestão de dados	Estabelecer e manter um processo de gestão de dados. No processo, tratar 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 organização. Revisar e atualizar a documentação anualmente ou quando ocorrerem mudanças significativas na organização que possam impactar esta medida de segurança.	1 2 3
3.2	Identificar	Estabelecer e manter um inventário de dados	Estabelecer e manter um inventário de dados, com base no processo de gestão de dados do órgão. No mínimo inventariar os dados sensíveis. Reavaliar e atualizar o inventário anualmente.	1 2 3
3.3	Proteger	Configurar listas de controle de acessos a dados	Aplicar listas de controle de acesso a dados, também conhecidas como permissões de acesso, a sistemas de arquivos, banco de dados e aplicações locais e remotos.	1 2 3
3.4	Proteger	Aplicar retenção de dados	Reter os dados de acordo com o processo de gestão de dados da organização. A retenção deve incluir prazos mínimos e máximos.	1 2 3
3.5	Proteger	Descartar dados com segurança	Descartar os dados com segurança, conforme processo de gestão de dados da organização. Certificar que o processo e método de descarte sejam compatíveis com a sensibilidade dos dados.	1 2 3
3.6	Proteger	Criptografar dados em dispositivos de usuário final	Criptografar os dados em dispositivos de usuário final que contenham dados sensíveis.	1 2 3
3.7	Identificar	Estabelecer e manter um esquema de classificação de dados	Estabelecer e manter um esquema geral de classificação de dados para o órgão, podendo ser "Sensíveis", "Confidencial" e "Público". Revisar e atualizar o esquema de classificação anualmente ou quando ocorrerem mudanças significativas que possam impactar essa medida de segurança.	2 3
3.8	Identificar	Documentar Fluxos de Dados	Documentar o fluxo de dados, contendo fluxos de dados do provedor de serviços, devendo ser baseada no processo de gestão de dados do órgão. Revisar e atualizar a documentação anualmente ou quando ocorrerem mudanças significativas que possam impactar essa medida de segurança	2 3
3.9	Proteger	Criptografar dados em mídia removível	Criptografar os dados em removível.	2 3
3.10	Proteger	Criptografar dados sensíveis em trânsito	Criptografar dados sensíveis em trânsito. Exemplos: <i>Transport Layer Security (TLS)</i> e <i>Open Secure Shell (Open SSH)</i>	2 3
3.11	Proteger	Criptografar dados sensíveis em repouso	Criptografar dados sensíveis em repouso em servidores, aplicações e banco de dados que contenham dados sensíveis.	2 3

3.12	Proteger	Segmentar o processamento e o armazenamento de dados com base na sensibilidade	Segmentar o processamento e armazenamento de dados com base na sensibilidade dos dados. Não processar dados sensíveis em ativos institucionais destinados a dados de menor sensibilidade.	2 3
3.13	Proteger	Implantar uma solução de prevenção contra perda de dados	Implementar uma ferramenta automatizada, de prevenção de perda de dados (DLP) baseada em host para identificar todos os dados sensíveis armazenados, processados ou transmitidos por meio de ativos institucionais.	3
3.14	Detectar	Registrar o acesso a dados sensíveis	Registrar o acesso a dados sensíveis, incluindo modificação e descarte.	3

Fique Atento!

Deve-se observar que não somente os dados sensíveis (conforme definição da LGPD), mas todos os dados pessoais possuem valor, e precisam de proteção. Assim, dados pessoais, e o seu subconjunto de dados pessoais sensíveis, devem ser protegidos contra violação de dados para dar adequada conformidade com a LGPD, observando-se em especial a legislação relativa a acesso, retenção e descarte dos dados.

CIS Controle 4: Configuração Segura de Ativos Institucionais e Software

Estabelecer e manter a configuração segura de ativos institucionais (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 implementar?

As configurações padrões para ativos e softwares institucionais são normalmente voltadas para a facilidade de implantação e uso, em vez da segurança. Controles básicos, serviços e portas abertos, contas ou senhas padrão e pré-instalação de software desnecessário podem ser explorados se deixados em seu estado padrão.

Referente às atualizações de configuração de segurança, elas precisam ser gerenciadas e mantidas ao longo do ciclo de vida dos ativos e software da instituição. Elas 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.

CIS Controle 4: Configuração segura de ativos institucionais e software

ID	NIST CSF	Medida de Segurança	Descrição da Medida de Segurança	Grupo de Implementação
4.1	Proteger	Estabelecer e manter um processo de configuração segura	Estabelecer e manter um processo de configuração segura para ativos institucionais e software. Revisar e atualizar a documentação anualmente ou quando ocorrerem mudanças significativas na organização que possam impactar esta medida de segurança.	1 2 3
4.2	Proteger	Estabelecer e Manter um Processo de Configuração Segura para a Infraestrutura de Rede	Estabelecer e manter um processo de configuração segura para dispositivos de rede. Revisar e atualizar a documentação anualmente ou quando ocorrerem mudanças significativas na organização que possam impactar esta medida de segurança.	1 2 3
4.3	Proteger	Configurar o bloqueio automático de sessão nos ativos	Configurar o bloqueio automático de sessão nos ativos 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.	1 2 3
4.4	Proteger	Implementar e gerenciar um firewall nos servidores	Implementar e gerenciar um firewall nos servidores, onde houver suporte.	1 2 3
4.5	Proteger	Implementar e gerenciar um firewall nos dispositivos de usuário final	Implementar e gerenciar 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.	1 2 3
4.6	Proteger	Gerenciar com segurança os ativos e software	Gerenciar com segurança os ativos e software. 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.	1 2 3
4.7	Proteger	Gerenciar contas padrão nos ativos e software	Gerenciar contas padrão nos ativos e software, como root, administrador e outras contas de fornecedores pré configuradas.	1 2 3
4.8	Proteger	Desinstalar ou desativar serviços desnecessários nos ativos e software	Desinstalar ou desativar serviços desnecessários nos ativos e software, como serviço de compartilhamento de arquivo não utilizado, módulo de aplicação web ou função de serviço.	2 3
4.9	Proteger	Configurar servidores DNS confiáveis nos ativos	Implementar configuração de ativos para usar servidores DNS controlados pelo órgão e/ou servidores DNS confiáveis acessíveis externamente.	2 3
4.10	Responder	Impor o bloqueio automático de dispositivos nos dispositivos portáteis do usuário final	Impor bloqueio automático de dispositivos quando houver um número pré-definido de tentativas de autenticação com falha,	2 3
4.11	Proteger	Impor a capacidade de limpeza remota nos dispositivos portáteis do usuário final	Limpar remotamente os dados institucionais de dispositivos portáteis de usuário final de propriedade da organização quando for considerado apropriado, como dispositivos perdidos ou roubados, ou quando um indivíduo não trabalha mais no órgão.	2 3

4.12	Proteger	Separar os Espaços de Trabalho nos dispositivos móveis	Certificar de que a separação de espaços de trabalho seja usada nos dispositivos móveis de usuário final, ou seja, separar aplicações e dados institucionais de aplicações e dados pessoais nos dispositivos, onde houver suporte	3
------	----------	--	---	---

CIS Controle 5: 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 institucionais de software.

Por que implementar?

É mais fácil para um agente de ameaça (externo ou interno) obter acesso não autorizado a ativos ou dados da organização usando credenciais de usuário válidas do que “hackeando” o ambiente. Existem várias formas de obter acesso a contas de usuário, podemos incluir:

- senhas fracas;
- contas ainda válidas depois que um colaborador deixa de trabalhar na organização;
- contas de teste;
- contas compartilhadas;
- contas de serviço incorporadas em aplicações para scripts;
- um usuário com a mesma senha que ele usa para uma conta online que foi comprometida (em um dump de senha pública);
- engenharia social em um usuário para fornecer sua senha;
- malware para capturar senhas ou tokens na memória ou na rede.

Contas administrativas ou com privilégio alto são alvos específicos porque permitem que atacantes adicionem outras contas ou façam alterações em ativos que podem torná-los mais vulneráveis a ataques. As contas de serviço também são sensíveis, pois geralmente são compartilhadas entre as equipes, internas e externas à organização, e às vezes desconhecidas, apenas para serem reveladas em auditorias de gestão de contas padrão.

CIS Controle 5: Gestão de contas

ID	NIST CSF	Medida de Segurança	Descrição da Medida de Segurança	Grupo de Implementação
5.1	Identificar	Estabelecer e manter um inventário de contas	Estabelecer e manter um inventário de todas as contas gerenciadas na organização. O inventário deve incluir contas de usuário e administrador. Validar se todas as contas ativas estão autorizadas, trimestralmente ou com mais frequência.	  
5.2	Proteger	Usar senhas exclusivas	Usar senhas exclusivas para todos os ativos institucionais. Contas que usam MFA (Autenticação multifator) no mínimo senhas de 8 caracteres e uma senha de 14 caracteres para contas que não usam o MFA.	  
5.3	Responder	Desabilitar contas inativas	Excluir ou desabilitar quaisquer contas inativas após um período de 45 dias de inatividade.	  
5.4	Proteger	Restringir privilégios de administrador a contas de Administrador dedicadas	Restringir os privilégios de administrador a contas de administrador dedicados nos ativos institucionais. Realizar 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.	  
5.5	Identificar	Estabelecer e manter um inventário de contas de serviço	Estabelecer e manter um inventário de contas de serviço. O inventário, no mínimo, deve conter o departamento proprietário, data de revisão e propósito. Realizar 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.	 
5.6	Proteger	Centralizar a gestão de contas	Centralizar a gestão de contas por meio de serviço de diretório ou de identidade	 

CIS Controle 6: 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 institucionais.

Por que implementar?

Deve ser assegurado que os usuários tenham acesso apenas aos dados ou ativos institucionais apropriados para suas funções e garantir 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.

CIS Controle 6: Gestão do controle de acesso

ID	NIST CSF	Medida de Segurança	Descrição da Medida de Segurança	Grupo de Implementação
6.1	Proteger	Estabelecer um Processo de Concessão de Acesso	Estabelecer e seguir um processo, de preferência automatizado, para conceder acesso aos ativos institucionais mediante nova contratação, concessão de direitos ou mudança de função de um usuário.	1 2 3
6.2	Proteger	Estabelecer um Processo de Revogação de Acesso	Estabelecer e seguir um processo, de preferência automatizado, para revogar o acesso aos ativos institucionais, 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.	1 2 3
6.3	Proteger	Exigir MFA para aplicações expostas externamente	Exigir que todas as aplicações corporativas ou de terceiros expostas externamente apliquem o MFA. Impor o MFA por meio de um serviço de diretório ou provedor de SSO é uma implementação satisfatória desta medida de segurança	1 2 3
6.4	Proteger	Exigir MFA para acesso remoto à rede	Exigir MFA para acesso remoto à rede.	1 2 3
6.5	Proteger	Exigir MFA para acesso administrativo	Exigir MFA para todas as contas de acesso administrativo, em todos os ativos institucionais, sejam gerenciados no site local ou por meio de um provedor terceirizado.	1 2 3
6.6	Identificar	Estabelecer e manter um inventário de sistemas de autenticação e autorização	Estabelecer e manter um inventário dos sistemas de autenticação e autorização da organização, incluindo aqueles hospedados no site local ou em um provedor de serviços remoto. Revisar e atualizar o inventário anualmente ou com mais frequência.	2 3
6.7	Proteger	Centralizar o controle de acesso	Centralizar o controle de acesso para todos os ativos institucionais por meio de um serviço de diretório ou provedor de SSO	2 3
6.8	Proteger	Definir e manter o controle de acesso baseado em funções	Definir e manter o controle de acesso baseado em funções, determinando e documentando os direitos de acesso necessários para cada função dentro da organização para cumprir com sucesso suas funções atribuídas. Realizar análises de controle de acesso de ativos institucionais para validar se todos os privilégios estão autorizados, em uma programação recorrente, uma vez por ano ou com maior frequência.	3

CIS Controle 7: Gestão Contínua de Vulnerabilidades

Desenvolva um plano para avaliar e rastrear vulnerabilidades continuamente em todos os ativos institucionais dentro da infraestrutura da organização, 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 implementar?

Compreender e gerenciar vulnerabilidades em uma rede corporativa é uma atividade contínua, que requer tempo, foco e recursos. Por isso, os defensores cibernéticos devem ter informações oportunas de ameaças disponíveis, tais como:

- Atualizações de software;
- Patches;
- Avisos de segurança;
- Boletins de ameaças;

Além de revisar regularmente seu ambiente para identificar essas vulnerabilidades antes que os atacantes o façam e explorem as mesmas para obter acesso ao ambiente.

CIS Controle 7: Gestão contínua de vulnerabilidades

ID	NIST CSF	Medida de Segurança	Descrição da Medida de Segurança	Grupo de Implementação
7.1	Proteger	Estabelecer e manter um processo de gestão de vulnerabilidade	Estabelecer e manter um processo de gestão de vulnerabilidade documentado para ativos institucionais. Revisar e atualizar a documentação anualmente ou quando ocorrerem mudanças significativas na organização	  
7.2	Responder	Estabelecer e manter um processo de remediação	Estabelecer e manter uma estratégia de remediação baseada em risco documentada em um processo de remediação, com revisões mensais ou mais frequentes.	  
7.3	Proteger	Executar a gestão automatizada de <i>patches</i> do sistema operacional	Realizar atualizações do sistema operacional em ativos institucionais por meio da gestão automatizada de <i>patches</i> mensalmente ou com mais frequência.	  
7.4	Proteger	Executar a gestão automatizada de <i>patches</i> de aplicações	Realizar atualizações de aplicações em ativos institucionais por meio da gestão automatizada de <i>patches</i> mensalmente ou com mais frequência.	  
7.5	Identificar	Realizar varreduras automatizadas de vulnerabilidade em ativos institucionais internos	Realizar varreduras automatizadas de vulnerabilidade em ativos institucionais internos trimestralmente ou com mais frequência. Realizar varreduras autenticadas e não autenticadas, usando uma ferramenta compatível com o SCAP(<i>Security Content Automation Protocol</i>).	 

7.6	Identificar	Realizar varreduras automatizadas de vulnerabilidade em ativos institucionais expostos externamente	Executar varreduras de vulnerabilidade automatizadas de ativos institucionais expostos externamente usando uma ferramenta de varredura de vulnerabilidade compatível com o SCAP. Executar varreduras mensalmente ou com mais frequência.	2 3
7.7	Responder	Corrigir vulnerabilidades detectadas	Corrigir as vulnerabilidades detectadas no software por meio de processos e ferramentas mensalmente, ou com mais frequentemente, com base no processo de correção.	2 3

CIS Controle 8: 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.

Por que implementar?

A coleta e análise de log são procedimentos críticos para que uma organização possa detectar atividades maliciosas rapidamente. Em certas ocasiões, os registros de auditoria são a única evidência de um ataque bem-sucedido. Durante a coleta do log deve-se ter o cuidado de coletar o mínimo de dados pessoais necessário para o desempenho das atividades de análise forense em incidentes de segurança, conforme preconiza a LGPD.

A gestão de registros de auditoria deve ser mantida em constante monitoração e uso, porque os atacantes sabem que muitas organizações mantêm logs de auditoria para fins de conformidade, entretanto raramente os analisam. Baseado nesse conhecimento, eles conseguem ocultar sua localização, um software malicioso ou atividades nas máquinas das vítimas. Caso os processos de análise de log sejam insatisfatórios ou inexistentes, os atacantes as vezes vão controlar as máquinas das vítimas por meses ou anos sem que sejam percebidos pela organização-alvo.

CIS Controle 8: Gestão de registros de auditoria

ID	NIST CSF	Medida de Segurança	Descrição da Medida de Segurança	Grupo de Implementação
----	----------	---------------------	----------------------------------	------------------------

8.1	Proteger	Estabelecer e manter um processo de gestão de log de auditoria	Estabelecer e manter um processo de gestão de log de auditoria que defina os requisitos de log da organização. Tratar da coleta, revisão e retenção de logs de auditoria para ativos institucionais. Revisar e atualizar a documentação anualmente ou quando ocorrerem mudanças significativas	1 2 3
8.2	Detectar	Coletar logs de auditoria	Coletar logs de auditoria. Certificar de que o log, de acordo com o processo de gestão de log de auditoria da organização, tenha sido habilitado em todos os ativos.	1 2 3
8.3	Proteger	Garantir o armazenamento adequado do registro de auditoria	Certificar de que os destinos dos logs mantenham armazenamento adequado para cumprir o processo de gestão de log de auditoria da organização.	1 2 3
8.4	Proteger	Padronizar a sincronização de tempo	Padronizar a sincronização de tempo. Configurar pelo menos duas fontes de tempo sincronizadas nos ativos institucionais.	2 3
8.5	Detectar	Coletar logs de auditoria detalhados	Configurar o log de auditoria detalhado para ativos institucionais contendo dados sensíveis. Incluir 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.	2 3
8.6	Detectar	Coletar logs de auditoria de consulta DNS	Habilitar o registro de log de consulta do servidor DNS (<i>Domain Name System</i>) para detectar pesquisas de nomes de host para domínios maliciosos conhecidos.	2 3
8.7	Detectar	Coletar logs de auditoria de requisição de URL	Coletar logs de auditoria de requisição de URL em ativos institucionais, quando apropriado e suportado.	2 3
8.8	Detectar	Coletar logs de auditoria de linha de comando	Habilitar o log de auditoria sobre ferramentas de linha de comando, tais como Microsoft Powershell e Bash.	2 3
8.9	Detectar	Centralizar os logs de auditoria	Centralizar a coleta e retenção de logs de auditoria nos ativos institucionais.	2 3
8.10	Proteger	Reter os logs de auditoria	Reter os logs de auditoria em ativos institucionais por no mínimo 90 dias.	2 3
8.11	Detectar	Conduzir revisões de log de auditoria	Realizar análises de logs de auditoria para detectar anomalias ou eventos anormais que possam indicar uma ameaça potencial. Realizar revisões semanalmente ou com mais frequência.	2 3
8.12	Detectar	Colete logs do provedor de serviços	Coletar logs do provedor de serviços. 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.	3

Fique Atento!

Ao coletar logs do provedor de serviço que tratam de dados pessoais deve-se observar as orientações contidas na LGPD e demais regulamentações de proteção de dados e privacidade pois a não conformidade pode acarretar em prejuízos financeiros e

reputacionais.

CIS Controle 9: 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.

Por que implementar?

Navegadores Web e clientes de e-mail são pontos de entrada muito comuns para atacantes em virtude de sua interação direta com usuários dentro das instituições.

Conteúdos podem ser criados para atrair ou enganar os usuários para que revelem suas credenciais, forneçam dados sensíveis ou forneçam um canal aberto onde os atacantes obtenham acesso, aumentando assim o risco para a corporação.

CIS Controle 9: Proteções de e-mail e navegador Web

ID	NIST CSF	Medida de Segurança	Descrição da Medida de Segurança	Grupo de Implementação
9.1	Proteger	Garantir o uso apenas de navegadores e clientes de e-mail suportados plenamente	Certificar de que apenas navegadores e clientes de e-mail suportados plenamente tenham permissão para executar na organização, usando apenas a versão mais recente dos navegadores e clientes de e-mail fornecidos pelo fornecedor.	1 2 3
9.2	Proteger	Usar serviços de filtragem de DNS	Usar os serviços de filtragem de DNS em todos os ativos institucionais para bloquear o acesso a domínios mal-intencionados conhecidos.	1 2 3
9.3	Proteger	Manter e impor filtros de URL baseados em rede	Impor e atualizar filtros de URL baseados em rede para limitar um ativo institucional de se conectar a sites potencialmente maliciosos ou não aprovados.	2 3
9.4	Proteger	Restringir extensões de cliente de e-mail e navegador desnecessárias ou não autorizadas	Restringir, seja desinstalando ou desabilitando, quaisquer plug-ins de cliente de e-mail ou navegador, extensões e aplicações complementares não autorizados ou desnecessários.	2 3
9.5	Proteger	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 <i>Sender Policy Framework (SPF)</i> e <i>DomainKeys Identified Mail (DKIM)</i> .	2 3

9.6	Proteger	Bloquear tipos de arquivo desnecessários	Bloquear tipos de arquivo desnecessários que tentem entrar no gateway de e-mail do órgão.	2 3
9.7	Proteger	Implantar e manter proteções antimalware de servidor de e-mail	Implantar e manter proteção <i>antimalware</i> de servidores de e-mail, como varredura de anexos e/ou <i>sandbox</i> .	3

CIS Controle 10: Defesas Contra Malware

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

Por que implementar?

O Malware, software malicioso geralmente classificado como vírus ou Trojans, está em constante evolução e adaptação. Os ataques ocorrem através de vulnerabilidades em dispositivos de usuário final e geralmente depende do comportamento inseguro do usuário, como clicar em links, abrir anexos, instalar software ou perfis, ou inserir unidade flash USB (Universal Serial Bus).

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 institucionais para detectar, impedir a propagação ou controlar a execução de software ou código malicioso.

CIS Controle 10: Defesas contra Malware

ID	NIST CSF	Medida de Segurança	Descrição da Medida de Segurança	Grupo de Implementação
10.1	Proteger	Instalar e manter um software anti-malware	Instalar e manter um software anti-malware em todos os ativos cibernéticos da organização.	1 2 3

10.2	Proteger	Configurar atualizações automáticas de assinatura anti-malware	Realizar a configuração de atualizações automáticas para as assinaturas anti-malware em todos os ativos cibernéticos da organização.	1 2 3
10.3	Proteger	Desabilitar a execução e reprodução automática para mídias removíveis	Configurar os dispositivos para a não execução e reprodução automática de mídias removíveis.	1 2 3
10.4	Detectar	Configurar a varredura anti-malware automática de mídia removível	Configure o software anti-malware para verificar automaticamente a mídia removível.	2 3
10.5	Proteger	Habilitar funções anti-exploração	Habilitar funcionalidades "anti-exploits" tais como Data Execution Prevention (DEP) ou Address Space Layout Randomization (ASLR) que estejam disponíveis no sistema operacional, ou implantar ferramentas apropriadas que possam ser configuradas para aplicar proteções sobre um conjunto mais amplo de aplicações e executáveis.	2 3
10.6	Proteger	Gerenciar o software anti-malware de maneira centralizada	Utilizar software anti-malware gerenciado centralmente para monitorar e defender continuamente cada uma das estações de trabalho e servidores da organização.	2 3
10.7	Detectar	Utilizar software anti-malware baseado em comportamento	Utilizar software anti-malware que consiga monitorar e identificar comportamentos fora do comum dos equipamentos da organização.	2 3

CIS Controle 11: Recuperação de Dados

Crie e mantenha práticas de recuperação de dados que sejam capazes de restaurar os ativos da organização para um estado pré-incidente ou o estado mais confiável possível.

Por que implementar?

Os órgãos 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 o órgão.

Quando os atacantes comprometem os ativos, fazem alterações nas configurações, adicionam contas e, frequentemente, adicionam softwares ou scripts, essas alterações nem sempre são fáceis de identificar, podendo incluir, adicionar ou alterar entradas de registro, abrir portas, desligar serviços de segurança, excluir logs ou outras ações maliciosas que tornam o sistema inseguro. Nem toda ação precisa ser

maliciosa; erros humanos também podem causar os mesmos danos. Portanto, é importante ter a capacidade de ter backups ou espelhos recentes para recuperar ativos e dados institucionais de volta a um estado confiável conhecido.

Vale ressaltar também o aumento exponencial de ransomware, caso em que o atacante realiza a criptografia dos dados de um órgão em uma forma de “sequestro” e em seguida exige um resgate para restauração ou para não divulgação e venda dos dados. Nesta situação, um backup recente seria útil para recuperar o sistema a um estado confiável, porém o risco de venda ou divulgação dos dados criptografados continuaria.

CIS Controle 11: Recuperação de dados

ID	NIST CSF	Medida de Segurança	Descrição da Medida de Segurança	Grupo de Implementação
11.1	Recuperar	Estabelecer e manter um processo de recuperação de dados	Estabelecer e manter um processo de recuperação de dados. Tal processo deve descrever em seu escopo as atividades de recuperação de dados, priorização da recuperação e a atividade de segurança dos dados de backup. Periodicamente, deve ser realizada uma revisão e/ou atualização deste processo, assim como em casos específicos quando ocorrerem mudanças significativas na organização que venham impactar a organização de forma significativa.	1 2 3
11.2	Recuperar	Executar backups automatizados	Garantir que todos os dados dos sistemas tenham cópias de segurança (backups) realizadas automaticamente e de forma regular.	1 2 3
11.3	Proteger	Proteger os dados de recuperação	Garantir que os dados de recuperação sejam protegidos adequadamente por meio de segurança física ou criptografia quando são armazenados, bem como quando são movidos pela rede. Isso inclui backups remotos e serviços em nuvem. Devem ser estabelecidos controles que garantam que os dados de recuperação sejam equivalentes aos dados originais.	1 2 3
11.4	Recuperar	Estabelecer e manter uma instância isolada de dados de recuperação	Criar e manter pelo menos uma instância isolada dos dados de recuperação. Alguns exemplos deste tipo de implementação são controle de versão de destinos de backup por meio de sistemas e serviços offline (backup offline, não acessível por meio de uma conexão de rede), em nuvem, ou em datacenter separado do site local.	1 2 3
11.5	Recuperar	Testar os dados de recuperação	Realizar o teste de integridade dos dados na mídia de backup regularmente, executando um processo de restauração de dados para garantir que o backup esteja funcionando corretamente.	2 3

CIS Controle 12: Gestão da Infraestrutura de Rede

Implemente e gerencie o ativo dos dispositivos de rede, com o objetivo de evitar que atacantes explorem serviços de rede e pontos de acesso vulneráveis.

Por que implementar?

Os órgãos 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 suporte do fornecedor para patches e atualizações de funcionalidades. Um diagrama de arquitetura de rede atualizado, incluindo o de segurança, é uma base importante para gestão de infraestrutura.

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 a fim de 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.

CIS Controle 12: Gestão da infraestrutura de rede

ID	NIST CSF	Medida de Segurança	Descrição da Medida de Segurança	Grupo de Implementação
12.1	Proteger	Garantir que a infraestrutura de rede esteja atualizada	Garantir que a infraestrutura de rede da organização esteja sempre atualizada. Deve ser realizada uma revisão das versões de software de forma periódica, ou quando for identificada uma vulnerabilidade que eleve o risco da organização.	1 2 3
12.2	Proteger	Garantir níveis de segurança para a arquitetura de rede	Garantir que a arquitetura de rede se mantenha segura. É interessante buscar implementar políticas de segurança como segmentação de rede, privilégio mínimo e níveis básicos de disponibilidade.	2 3
12.3	Proteger	Gerenciar infraestrutura de rede e segurança	Implementar e gerenciar com segurança a infraestrutura de rede da organização.	2 3
12.4	Identificar	Elaborar e manter diagramas de arquitetura	Elaborar e manter diagramas e demais documentações da arquitetura de rede da organização. A revisão destas documentações deve ser realizada de forma periódica ou quando ocorrerem mudanças que possam impactar tais artefatos.	2 3
12.5	Proteger	Centralizar a autenticação, autorização e auditoria de rede (AAA)	Implementar a centralização de (AAA) de rede.	2 3

12.6	Proteger	Utilizar protocolos de comunicação e gestão de rede seguros	Implementar protocolos de comunicação e rede seguros.	2 3
12.7	Proteger	Garantir que os dispositivos remotos utilizem uma VPN e se conectem em uma infraestrutura AAA segura da organização	Fazer com que os usuários se autentiquem em serviços de autenticação e VPN gerenciados pela organização antes de acessar os dispositivos e recursos da organização.	2 3
12.8	Proteger	Utilizar e manter recursos cibernéticos dedicados para todo o trabalho administrativo	Habilitar a coleta de Netflow e registros de log em cada um dos dispositivos existentes Para a execução de tarefas administrativas, utilize e mantenha recursos cibernéticos dedicados, estes devem estar fisicamente ou logicamente separados e seguros. É importante que tais recursos sejam segmentados da rede primária da organização, e não deve ser permitido o acesso a rede externa da organização. fronteiras da rede.	3

CIS Controle 13: Monitoramento e Defesa da Rede

Implementar processos e ferramentas para que assim a organização seja capaz de estabelecer o monitoramento e a defesa de rede contra ameaças de segurança em toda a sua infraestrutura de rede e base de usuários.

Por que implementar?

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.

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.

Pode ocorrer de um órgão estar comprometido por semanas, meses ou anos antes de ser descoberto. 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 do órgão.

CIS Controle 13: Monitoramento e defesa da Rede

ID	NIST CSF	Medida de Segurança	Descrição da Medida de Segurança	Grupo de Implementação
13.1	Detectar	Centralizar alertas de eventos de segurança	Centralize os alertas de eventos de segurança em ativos institucionais para que a organização consiga realizar a correlação e análise do log. Uma boa prática é o uso de um SIEM que inclua alertas de correlação de eventos definidos pelo fornecedor. Outra boa prática é a adoção de uma plataforma de análise de log configurada com aletas de correlação relevantes para a segurança cibernética.	1 2 3
13.2	Detectar	Implantar soluções de detecção e intrusão baseada em host.	Implante soluções para detecção de intrusão baseada em host em ativos institucionais	2 3
13.3	Detectar	Implantar soluções de detecção e intrusão baseada em rede	Implante soluções para detecção de intrusão de rede em ativos institucionais	2 3
13.4	Proteger	Realizar filtragem de tráfego entre os segmentos de rede	Realize a filtragem de tráfego entre os segmentos de rede.	2 3
13.5	Proteger	Aplicar o gerenciamento de controle de acesso em ativos remotos	Aplique o gerenciamento de controle de acesso em ativos que se conectam remotamente a organização. Determine a quantidade de acesso aos recursos da organização utilizando softwares anti-malware devidamente atualizados, processos de configuração segura de ativos e certifique-se que os sistemas operacionais e demais aplicações estejam sempre atualizados.	2 3
13.6	Detectar	Coletar logs de fluxo e tráfego de rede	Realize a coleta dos logs de fluxo e tráfego de rede com o objetivo de checar e alertar sobre dispositivos de rede que estejam com comportamento que fujam do padrão, em sua necessidade de acesso como parte de suas responsabilidades.	2 3
13.7	Proteger	Implantar soluções para prevenção de intrusão baseada em host	Implante uma solução para prevenção de intrusão baseada em host e ativos institucionais, preferencialmente com suporte do fornecedor.	3
13.8	Proteger	Implantar soluções para prevenção de intrusão de rede	Implante uma solução para prevenção de intrusão baseada em rede, preferencialmente com suporte do fornecedor.	3
13.9	Proteger	Implantar controle de acesso a nível de porta	Implante o controle de acesso em nível de porta. Tal controle utiliza o protocolo 802.1x ou soluções semelhantes como certificados, também podem ser utilizadas ferramentas para autenticação de usuário e/ou dispositivo.	3
13.10	Proteger	Realizar a filtragem de camada de aplicação	Realize a filtragem de camada de aplicação. Exemplos de implementações são proxy de filtragem, firewall desta camada ou gateway.	3
13.11	Detectar	Ajustar limites de aletas de eventos de segurança	Ajuste periodicamente os limites dos alertas de eventos de segurança.	3

CIS Controle 14: Conscientização e Treinamento de Competências sobre Segurança

Implantar e manter um programa de conscientização de segurança que possa

influenciar e conscientizar o comportamento dos colaboradores, tornando-os devidamente qualificados e assim atingir o objetivo de reduzir riscos de segurança cibernética da organização.

Por que implementar?

As ações das pessoas podem causar incidentes, intencionalmente ou não. É mais fácil induzir um usuário a clicar em um link ou abrir um anexo de e-mail para instalar malware e entrar na rede uma organização, do que fazer um exploit de rede diretamente. Nenhum programa de segurança pode lidar com o risco cibernético de maneira eficaz sem um meio de lidar com essa vulnerabilidade humana fundamental. Cada usuário do órgão em qualquer nível tem riscos diferentes.

Os treinamentos e conscientizações devem ser atualizados regularmente. Isso aumentará a cultura de segurança.

CIS Controle 14: Conscientização e treinamento de competências sobre segurança

ID	NIST CSF	Medidas de Segurança	Descrição da Medida de Segurança	Grupo de Implementação
14.1	Proteger	Implantar e manter um programa de conscientização de segurança	Criar programa de conscientização de segurança para que todos os membros da força de trabalho o realizem regularmente com o objetivo de garantir que eles entendam e exibam os conhecimentos e comportamentos necessários para ajudar a garantir a segurança da instituição. O programa de conscientização de segurança da instituição deve ser comunicado de maneira contínua e envolvente.	  
14.2	Proteger	Treinar colaboradores para reconhecer ataques de engenharia social	Treinar os colaboradores sobre como identificar diferentes formas de ataques de engenharia social, como phishing, golpes de telefone e chamadas realizadas por impostores.	  
14.3	Proteger	Treinar os colaboradores nas melhores práticas de autenticação	Treinar os colaboradores sobre a importância de habilitar utilizar as melhores práticas de autenticação segura como MFA (Multi-factor Authentication – Autenticação de múltiplos fatores), composição de senha e gestão de credenciais.	  
14.4	Proteger	Treinar os colaboradores nas Melhores Práticas de Tratamento de Dados.	Treinar os membros da força de trabalho sobre como identificar e armazenar, transferir, arquivar e destruir informações sensíveis (incluindo dados pessoais) adequadamente. Isto também inclui o treinamento sobre práticas recomendadas de mesa e tela limpas, (não deixar senhas expostas nas mesas de trabalho e bloquear a tela da estação de trabalho ao se ausentar), apagar quadros físicos e virtuais após reuniões e armazenar dados e ativos com segurança.	  

14.5	Proteger	Treinar os colaboradores sobre as causas da exposição não intencional de dados	Treinar os membros da força de trabalho para estarem cientes das causas de exposições de dados não intencionais, como perder seus dispositivos móveis ou enviar e-mail para a pessoa errada devido ao preenchimento automático de e-mail.	1 2 3
14.6	Proteger	Treinar os colaboradores sobre o Reconhecimento e Comunicação de Incidentes de Segurança	Treinar os colaboradores para serem capazes de identificar os indicadores mais comuns de um incidente e serem capazes de relatar tal incidente.	1 2 3
14.7	Proteger	Treinar os colaboradores sobre como identificar e comunicar se os seus ativos institucionais estão com desatualizados em relação a segurança	Treine os colaboradores para entender como verificar e relatar patches de software desatualizados ou quaisquer falhas em ferramentas e processos automatizados. É importante incluir nesse treinamento a etapa de notificação do pessoal de TI sobre quaisquer falhas em processos e ferramentas automatizadas que estejam ocorrendo.	1 2 3
14.8	Proteger	Treinar os colaboradores sobre os perigos de se conectar e transmitir dados institucionais em redes inseguras	Treine os colaboradores sobre os perigos de se conectar e transmitir dados em redes inseguras para atividades corporativas. Se a organização tiver funcionários remotos, o treinamento deve incluir orientação para garantir que todos os usuários configurem com segurança sua infraestrutura de rede doméstica.	1 2 3
14.9	Proteger	Conduzir treinamento de competências e conscientização de segurança para funções específicas	Para colaboradores que atuem em funções específicas, realize o treinamento de conscientização de segurança e de competências específicas para estas 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 e treinamento avançado de conscientização de engenharia social para funções de níveis estratégico da organização	2 3

CIS Controle 15: Gestão de Provedor de Serviços

Com o objetivo de garantir a proteção das informações, sistemas e processos críticos da organização, estabeleça um processo para avaliar os provedores de serviços que operem e mantenham estes ativos da organização.

Por que implementar?

Normalmente as organizações contam com fornecedores e parceiros para ajudar a gerenciar seus dados ou contam com infraestrutura de terceiros para aplicações ou funções essenciais.

Violações de terceiros costumam impactar significativamente uma organização, como por exemplo os ataques de ransomware que podem ser realizados indiretamente, quando há um bloqueio de um de seus provedores de serviço, causando a interrupção nos negócios, ou diretamente, criptografando os dados da organização.

A maioria das regulamentações de segurança e privacidade de dados exige que sua proteção seja estendida a prestadores de serviços terceirizados. A confiança de terceiros é uma função central de Governança, Riscos e Compliance (GRC), pois os riscos que não são gerenciados dentro da organização são transferidos para entidades fora da organização.

Além disso, 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 organização tem um “checklist” diferente ou conjunto de padrões para classificar o provedor de serviços. As seguradoras que vendem apólices de segurança cibernética também têm suas próprias medidas.

CIS Controle 15: Gestão de Provedor de Serviços

ID	NIST CSF	Medida de segurança	Descrição da Medida de Segurança	Grupo de Implementação
15.1	Identificar	Criar e gerenciar o inventário de provedores de serviços	Crie e gerencie o inventário de provedores de serviços. Este inventário deve listar todos os provedores de serviços da organização, incluir classificações, e conter contatos institucionais para cada provedor de serviço. Deve ser realizada uma revisão e/ou atualização deste inventário anualmente ou quando ocorrerem mudanças significativas do provedor que venham impactar a organização de forma significativa.	  
15.2	Identificar	Criar e gerenciar uma política de gestão de provedores de serviços	Crie e gerencie uma política de gestão de provedores de serviços. Faça com que tal política trate de classificação, inventário, avaliação, monitoramento e descomissionamento de prestadores e provedores de serviço da organização. Deve ser realizada uma revisão e/ou alteração desta política periodicamente, em casos específicos quando ocorrerem mudanças significativas na organização que venham impactar a organização de forma significativa.	 
15.3	Identificar	Classificar provedores de serviços.	Realize a classificação de provedores de serviços. Para que seja realizada a classificação podem ser levadas em consideração uma ou mais característica do provedor, como a sensibilidade dos dados e informações que este provedor opera/gerencia, volume destes dados e informações, regulamentações aplicáveis, requisitos de disponibilidade e classificação de risco. Deve ser realizada uma revisão e/ou alteração desta classificação periodicamente, em casos específicos quando ocorrerem mudanças significativas na organização que venham impactar a organização e forma significativa	 
15.4	Proteger	Garantir que os contratos dos provedores de serviços contenham requisitos mínimos de segurança	Faça com que os contratos do provedor de serviços contenham requisitos de segurança, alguns exemplos destes requisitos de segurança são, requisitos mínimos de segurança do software, resposta a incidentes de segurança, criptografia e descarte de dados. Tais requisitos mínimos devem ser concisos com a política de gestão de provedores da organização. Deve ser realizada uma revisão dos contratos de provedores de forma periódica com o objetivo de atualizar e garantir que os requisitos de segurança estão sendo cumpridos.	 

15.5	Identificar	Avaliar provedores de serviços	Realizar a avaliação de provedores de serviços da organização. O escopo da avaliação deve levar em consideração as diretrizes contidas na política de gestão de provedores de serviços além de classificações e relatórios de avaliação padronizados, questionários, e processos rigorosos aplicáveis. A avaliação de provedores de serviço deve ser realizada de forma periódica e na medida em que novos contratos estipulados ou renovados.	3
15.6	Detectar	Monitorar provedores de Serviço	Realizar a monitoração de provedores de acordo com a política de gestão dos provedores de serviços. Tal monitoração pode incluir a avaliação periódica do provedor, monitoração de artefatos entregues pelo provedor	3
15.7	Proteger	Encerrar de forma segura o contrato com o provedor de serviços	Realizar de forma segura o encerramento de contrato de provedores e prestadores de serviço. Algumas ações que possam ser utilizadas para realizar o encerramento de contratos ou desligamento de prestadores são, desativação de contas de usuário e serviço utilizadas durante o contrato, encerramento de fluxo de dados e descarte seguros de dados e informações corporativas em sistemas dos provedores de serviço.	3

CIS Controle 16: Segurança de Aplicações

Gerenciar o ciclo de vida de segurança de todos os softwares desenvolvidos e adquiridos internamente, a fim de prevenir, detectar e corrigir falhas de segurança.

Por que implementar?

As organizações usam aplicações para gerenciar seus dados mais sensíveis e controlar o acesso aos recursos do sistema. Na ausência de credenciais, 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.

As aplicações de hoje são desenvolvidas, operadas e mantidas em um ambiente altamente complexo, diverso e dinâmico, sendo 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.

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, hoje em dia 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 organizações 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 organizações que estendem essas aplicações devem seguir este Controle CIS, semelhante a se estivessem fazendo o desenvolvimento de cliente desde o início.

CIS Controle 16: Segurança de Aplicações

ID CSF	NIST	Medida de Segurança	Descrição da Medida de Segurança	Grupo de Implementação
16.1	Proteger	Estabelecer e manter um processo de desenvolvimento de aplicações	Estabelecer e manter um processo de desenvolvimento de aplicações seguro. Este processo deve tratar de itens como padrões de design seguro de aplicações (Security by Design), práticas de codificação seguras, treinamentos para desenvolvedores, gestão de vulnerabilidades, segurança de código de terceiros e procedimentos de teste de segurança de aplicação. Deve ser realizada uma revisão e/ou alteração deste processo periodicamente, em casos específicos ou quando ocorrerem mudanças na organização que venham impactá-la de forma significativa.	2 3
16.2	Proteger	Estabelecer e manter um processo para aceitar e endereçar vulnerabilidades de software	Estabelecer e manter um processo de aceitação e tratamento de informações sobre vulnerabilidades de software, incluindo mecanismos para que entidades externas contactem o grupo de segurança da instituição. É importante que o processo inclua itens como: Política de tratamento de vulnerabilidades identificadas e relatadas, equipe ou profissional responsável por analisar os	2 3

			relatórios de vulnerabilidade e um processo de entrada, atribuição, correção e testes de correção. Como parte deste processo, é importante rastrear as vulnerabilidades, classificar a gravidade e atribuir métricas capazes de medir o tempo de identificação, análise e correção das vulnerabilidades. Deve ser realizada uma revisão e/ou alteração deste processo periodicamente, em casos específicos ou quando ocorrerem mudanças na organização que venham impactá-la de forma significativa	
16.3	Proteger	Executar análise de causa raiz em vulnerabilidades de segurança	Executar a análise de causa raiz em vulnerabilidades de segurança. A análise da causa raiz é a tarefa capaz de avaliar os problemas subjacentes que criam vulnerabilidades no código da aplicação e permite que as equipes de desenvolvimento vão além de apenas corrigir vulnerabilidades individuais conforme elas surgem	23
16.4	Proteger	Estabelecer e gerenciar um inventário de componentes de software de terceiros	Estabelecer e gerenciar 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 a organização. Deve ser realizada uma revisão e/ou alteração deste inventário periodicamente, com o objetivo de identificar quaisquer mudanças ou atualização nesses componentes e validar a compatibilidade do mesmo.	23
16.5	Proteger	Usar componentes de software de terceiros atualizados e confiáveis	Utilizar apenas componentes de terceiros atualizados e confiáveis. Quando possível, escolher bibliotecas e estruturas pré-estabelecidas e comprovadas que forneçam a segurança adequada. É importante adquirir tais componentes de fornecedores e fontes confiáveis ou realizar a avaliação de vulnerabilidades do software antes de usar/adquirir	23
16.6	Proteger	Estabelecer e manter um processo para a classificação de gravidade de vulnerabilidades	Estabelecer e manter um processo para a classificação de gravidade de vulnerabilidades capaz de facilitar a priorização na medida em que as vulnerabilidades descobertas são corrigidas. Esse processo deve incluir a definição de um nível mínimo de aceitabilidade de segurança para a liberação de código ou aplicações. A classificação de gravidade deve trazer uma forma sistemática de triagem de vulnerabilidades que venha a melhorar a gestão de riscos e ajuda a garantir que os bugs mais graves sejam priorizados. Revise o processo e a classificação de vulnerabilidade periodicamente.	23
16.7	Proteger	Usar modelos de configurações de segurança padrão para infraestrutura de aplicações	Utilizar modelos de configuração de segurança padrão (Segurança by Default) recomendados pela equipe de segurança em 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 Security as a Service (SaaS). Não permita que o software desenvolvido internamente enfraqueça as configurações de segurança da organização.	23
16.8	Proteger	Separar sistemas de produção e não produção	Manter ambientes separados para sistemas de produção e não produção.	23
16.9	Proteger	Treinar desenvolvedores em conceitos de segurança de aplicações e codificação segura	Garantir que todos os responsáveis pelo desenvolvimento de software recebam treinamento para escrever código seguro para seu ambiente de desenvolvimento e responsabilidades específicas. O treinamento deve incluir princípios gerais de segurança e práticas padrão de segurança para aplicações. O treinamento deve ser realizado periodicamente, é interessante estabelecer uma cultura de segurança entre os desenvolvedores.	23
16.10	Proteger	Aplicar princípios de design seguro em arquiteturas de aplicações	Aplicar 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.	23

16.11 Proteger	Aproveitar os módulos ou serviços controlados para componentes de segurança de aplicações	Aproveitar módulos ou serviços controlados para componentes de segurança da aplicação, como gestão de identidade, criptografia e auditoria de logs. O uso de recursos para plataforma em funções críticas de segurança deve reduzir a carga de trabalho dos desenvolvedores e minimizar 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.	2 3
16.12 Proteger	Implementar verificações de segurança em nível de código	Utilizar ferramentas de análise estáticas e dinâmicas dentro do ciclo de vida da aplicação para verificar se as práticas de codificação seguras estão sendo utilizadas na organização.	3
16.13 Proteger	Realizar teste de invasão de aplicação	Realizar testes de invasão em aplicações. Para aplicações críticas, o teste de invasão autenticado é mais adequado para localizar vulnerabilidades de codificação e 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 uma aplicação como um usuário autenticado e não autenticado.	3
16.14 Proteger	Realizar aplicações de modelagem de ameaças	Realizar 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 desenho, antes que o código seja criado. É conduzido por profissionais especialmente treinados 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 todos os pontos fracos.	3

CIS Controle 17: Gestão de Resposta a Incidentes

Proteja as informações e a reputação da organização, desenvolvendo e implementando uma infraestrutura de resposta a incidentes (por exemplo: planos, definição de papéis, treinamento, comunicações, gerenciamento de supervisão) para descobrir um ataque de forma ágil, e depois, conter efetivamente o impacto, eliminar a presença do atacante, e restaurar a integridade da rede e dos sistemas da organização.

Por que implementar?

Um programa abrangente de segurança cibernética inclui proteções, detecções, resposta e recursos de recuperação. Frequentemente, os dois últimos são esquecidos em organizações 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 organização, responder a elas antes que possam se espalhar e remediá-las antes que possam causar danos. É necessário entender todo o escopo de um incidente, como aconteceu e o que pode ser feito para

evitar que aconteça novamente, com o objetivo de solucionar o incidente de forma eficiente.

Não podemos esperar que nossas proteções sejam eficazes 100% do tempo. Quando ocorre um incidente, se uma organização 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 organização 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 organização 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 organização. 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 organização, 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.

CIS Controle 17: Gestão de resposta a incidentes

ID CSF	NIST	Medida de Segurança	Descrição da Medida de Segurança	Grupo de Implementação
17.1	Responder	Designar os colaboradores para gerenciar o tratamento de incidentes	Designar os responsáveis para gerenciar o processo de tratamento de incidentes da organização. A equipe de gestão é responsável pela coordenação e documentação dos esforços de resposta e recuperação a incidentes, esta equipe pode formada por colaboradores internos, terceirizados ou pode contar com os dois tipos de colaboradores. Casos em que a equipe for composta somente por funcionários terceirizados, a organização deve designar pelo menos um colaborador interno para supervisionar qualquer ação terceirizada.	

17.2	Responder	Estabelecer e manter informações de contato para relatar incidentes de segurança	Estabelecer e manter as informações de contato das pessoas 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 periodicamente para garantir que as informações estejam atualizadas.	  
17.3.	Responder	Estabelecer e manter um processo institucional para relatar incidentes	Estabelecer e manter um processo institucional para a colaborares relatarem incidentes de segurança. O processo inclui cronograma de relatórios, pessoal responsável por para relatar, mecanismo para relatar e as informações mínimas a serem relatadas. É importante certificar que o processo está publicamente disponível para todos os colaboradores da organização. Deve ser realizada uma revisão periódica deste processo ou quando ocorrerem mudanças significativas na organização que possam impactar esta medida de segurança.	  
17.4	Responder	Estabelecer e manter um processo de resposta a incidente	Estabelecer e manter um processo de resposta a incidentes que aborde funções e responsabilidades, requisitos de conformidade e um plano de comunicação. Realize a revisão deste processo de forma periódica ou quando ocorrerem mudanças significativas na organização que possam impactar esta medida de segurança.	 
17.5	Responder	Atribuir funções e responsabilidades chave	Atribuir funções e responsabilidades chave para resposta a incidentes, incluindo equipe jurídica, TI, segurança da informação, instalações, relações públicas, recursos humanos, equipe de resposta a incidentes, conforme aplicável. Realize a revisão deste processo de forma periódica ou quando ocorrerem mudanças significativas na organização que possam impactar esta medida de segurança. Realize a revisão desta medida de forma periódica ou quando ocorrerem mudanças significativas na organização que possam impactar esta medida de segurança.	 
17.6	Responder	Definir mecanismos de comunicação durante a resposta a incidente	Determinar quais mecanismos primários e secundários serão usados para relatar um incidente e se comunicar 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. Realize a revisão desta medida de forma periódica ou quando ocorrerem mudanças significativas na organização que possam impactar esta medida de segurança.	 
17.7	Recuperar	Conduzir exercícios de resposta a incidentes rotineiros	Planejar e conduzir exercícios e cenários rotineiros de resposta a incidentes para a equipe envolvida na resposta a incidentes, de forma a manter a conscientização e tranquilidade no caso de resposta a ameaças reais. Os exercícios devem testar os canais de comunicação, tomada de decisão e recursos técnicos da equipe de resposta a incidentes, contemplando a utilização das ferramentas e dados disponíveis.	 
17.8.	Recuperar	Realizar análises pós-incidente	Realizar 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.	 
17.9	Recuperar	Estabelecer e manter limites de incidentes de segurança	Estabelecer 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, ameaça de segurança, violação de dados, incidente de privacidade etc. Realize a revisão desta medida de forma periódica ou quando ocorrerem mudanças significativas na organização que possam impactar esta medida de segurança.	

Fique Atento!

A Secretaria de Governo Digital disponibiliza em seu portal um Guia de

Resposta a Incidentes de Segurança, com enfoque em incidentes que envolvam dados pessoais, que constitui referência importante para instituições e profissionais de segurança da informação, que desejam realizar o tratamento de incidentes cibernéticos.

É importante lembrar também, que incidentes de segurança que envolvam dados pessoais sensíveis ou não carecem de procedimentos específicos estabelecidos na LGPD e seu descumprimento pode levar a sanções pela ANPD.

Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_resposta_incidentes.pdf

CIS Controle 18: Testes de Invasão

Teste a eficácia e a resiliência dos ativos institucionais através da identificação e exploração de fraquezas nos controles de segurança e da simulação das ações e objetivos de um atacante.

Por que implementar?

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 organizações 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 organização.
- Como um meio de testar o funcionamento correto das defesas da organização (“verificação”).
- Para testar se a organização 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 institucionais e humanos, e a eficácia das defesas e controles de mitigação para proteger contra impactos adversos para a organização. 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.

CIS Controle 18: Testes de Invasão

ID	NIST CSF	Medida de Segurança	Descrição da Medida de Segurança	Grupo de Implementação
18.1	Identificar	Elaborar e manter um programa de teste de invasão	Estabelecer um programa para testes de invasão adequado ao tamanho, complexidade e maturidade da organização. O programa de teste de invasão deve levar em consideração o escopo do teste como rede, aplicação web, API, controles de instalações físicas e etc.	2 3
18.2	Identificar	Realizar testes de invasão externos periódicos	Conduzir testes de invasão e externos regularmente. A teste de invasão externo deve ser reconhecido pela organização e deve ser capaz de detectar informações exploráveis que possam impactar a segurança da organização. Tal teste deve ser realizado por profissionais qualificados.	2 3
18.3	Proteger	Corrigir as descobertas do teste de invasão	Corrigir as descobertas do teste de invasão com base na política da organização para o escopo e a priorização de correção de vulnerabilidades.	2 3
18.4	Proteger	Validar as medidas de segurança	Validar as medidas de segurança após cada teste de invasão. Se necessário, modificar os conjuntos de regras e recursos para detectar as técnicas usadas durante o teste.	3
18.5	Identificar	Realizar testes de invasão internos periódicos	Realize testes de invasão internos periódicos com base nos requisitos do programa de testes de invasão.	3

4 - Ferramenta de Acompanhamento da Implementação dos Controles do CIS

A ferramenta em planilha utilizada para o acompanhamento da implementação dos controles do CIS é uma adaptação da ferramenta disponibilizada pela instituição AuditScripts à comunidade de segurança. O conteúdo foi adaptado para o presente framework, a organização da planilha foi ajustada para melhor apresentar a

necessidade da organização, mas os cálculos foram mantidos.

Ao usar a ferramenta para auxiliar na implementação dos controles do CIS, a instituição interessada deverá atentar ainda para o Grupo de Implementação (1, 2 ou 3) ao qual pertence, conforme explicado no Capítulo 1. A utilização da ferramenta sugerida pelo presente guia constitui apenas um apoio complementar na implementação. Sua utilização não representa, por si só, conformidade integral aos controles, que deverão ser verificados e comprovados individualmente, item por item, com referência direta à documentação oficial do CIS.

4.1 Estrutura e Organização da Ferramenta

A ferramenta possui cinco tipos de planilhas:

Planilha	Função
Leia-me	Apresenta informações gerais sobre a planilha, organização e definição dos campos.
Dashboard	Apresenta um painel gerencial com resumos gráficos das principais informações preenchidas nos 18 controles, como: porcentagem de implementação dos controles, porcentagem por grupo do NIST CSF, por grupo de implementação, entre outros.
CSC #1 a CSC #18	Cada uma das planilhas apresenta as medidas de segurança de um determinado controle, conforme distribuição do CIS.
Valores	Representa a base de informações para respostas de status de um determinado controle. Recomenda-se não alterar os valores presentes nessa planilha, pois invalidará cálculos que a planilha realiza.
Adaptações	Apresenta as adaptações realizadas nesse framework para atender a necessidade da organização.

Abaixo são descritos os campos que são encontrados nas planilhas:

Campos	Função
--------	--------

ID	Este é o número de identificação (ID) da medida de segurança e a vincula a cada um dos 18 Controles de Segurança Crítico, adaptada da documentação CIS-Controls-Version-8.
Detalhamento do Controle de Segurança Crítico	Este campo detalha cada medida de segurança específica, adaptada da documentação CIS-Controls-Version-8.
NIST CSF	Representa a atuação do controle em um uma das Funções da Estrutura Básica do NIST Framework for Improving Critical Infrastructure Cybersecurity (Identificar, Detectar, Proteger, Responder e Recuperar).
Linha de Base	Indica a ação da medida de segurança para basilar a implementação.
Política Aprovada	Indica se a instituição tem uma política definida que aponta que eles devem implementar a medida de segurança definida.
Controle Implementado	Determina se a instituição atualmente implementou ou não a medida de segurança e em que grau o controle foi implementado.
Controle Automatizado	Determina se a instituição atualmente automatizou ou não a implementação desta medida de segurança, e em que grau o controle foi automatizado.
Controle Reportado à Direção	Determina se os responsáveis pela implementação estão reportando esta medida de segurança aos representantes da alta direção, e em que grau o controle foi reportado.
Medida de Segurança Adequadas	Concentra informações sobre a adequação de um controle em um índice, em que, quanto mais próximo de 0%, menos adequado as medidas de segurança estão e, quanto mais próximo de 100%, mais adequados estão. As informações concentradas retratam o status das medidas de segurança presentes em uma política definida, seu status de implementação, seu status de automatização ou imposição técnica e o reporte à alta direção.
Medida de Segurança Não Adequadas	Concentra informações sobre a não adequação de um controle em um índice, em que quanto mais próximo de 0%, mais adequados as medidas de segurança estão e, quanto mais próximo de 100%, menos adequados estão. As informações concentradas retratam o status das medidas de segurança presentes em uma política definida, seu status de implementação, seu status de automatização ou imposição técnica e o reporte à alta direção.

Grupo de Implementação	Cada um dos três grupos possui atributos específicos que devem ser atendidos. Entretanto, a cada grupo avançado, os atributos são acumulados, ou seja, o grupo de implementação 2 tem incluso o grupo de implementação 1 e o grupo de implementação 3 tem inclusos os grupos de implementação 1 e 2.
------------------------	--

4.2 Níveis de Maturidade e demais Cálculos

A planilha é estruturada em 5 níveis de maturidade. Cada nível consiste em aspectos diferentes da adequação dos controles do CIS, que somados, resultam no índice de maturidade. As tabelas a seguir apresentam os cinco níveis, o índice de maturidade e uma descrição do que cada um deles aborda:

Nível de Maturidade	Descrição	Descrição detalhada da pontuação
1	Políticas Publicadas	Quanto mais próxima a pontuação é de um, maior é a maturidade da instituição na criação, padronização e divulgação de processos seguros.
2	Controles 1 a 5 Implementados	Quanto mais próximo o índice é de um, maior a adequação dos controles de 1 a 5.
3	Todos os Controles Implementados	Quanto mais próxima a pontuação é de um, maior a adequação dos controles de 6 a 18.
4	Todos os Controles Automatizados	Quanto mais próximo a pontuação é de um, maior a independência humana da execução dos controles.
5	Todos os Controles Reportados	Quanto mais próxima a pontuação é de um, maiores são a ciência e o comprometimento da alta direção com os processos de segurança.

Informações sobre o Índice de Maturidade:

Nível	Descrição	Descrição detalhada da pontuação
Índice de Maturidade	Índice expresso em escala de 0 a 5.	O Índice é o somatório de todas as pontuações de níveis de maturidade. Pontuação Nível 1 + Pontuação Nível 2 + Pontuação Nível 3 + Pontuação Nível 4 + Pontuação Nível 5 = Índice de Maturidade Quanto mais próxima de 1 for a pontuação de cada nível, maior será a maturidade da instituição em segurança da informação.

A maioria das medidas de segurança é avaliada pelo responsável nos seguintes aspectos: **Política Aprovada**, **Controle Implementado**, **Controle Automatizado** e **Controle Reportado à Direção**. Cada um deles possui respostas específicas de acordo com a situação momentânea do quesito avaliado. Tais respostas têm pesos que variam de 0 a 1. A tabela abaixo ilustra o que foi mencionado:

Respostas possíveis para cada uma das medidas de segurança				
Política Aprovada	Controle Implementado	Controle Automatizado	Controle Reportado à Direção	Peso
Sem Política	Não Implementado	Não Automatizado	Não Reportada	0
Política Informal	Partes da Política Implementadas	Partes da Política Automatizadas	Partes da Política Reportadas	0,25

Política Parcialmente Escrita	Implementada em Alguns Sistemas	Automatizada em Alguns Sistemas	Reportada em Alguns Sistemas	0,50
Política Escrita	Implementada em Muitos Sistemas	Automatizada em Muitos Sistemas	Reportada em Muitos Sistemas	0,75
Política Aprovada	Implementada em Todos os Sistemas	Automatizada em Todos os Sistemas	Reportada em Todos os Sistemas	1

Os níveis de maturidade são calculados a partir de cada uma das respostas. Basicamente, é realizada uma média dos pesos (respostas obtidas) em cima da quantidade de medidas de segurança daquele nível avaliado. A tabela abaixo simula, apenas como exemplo prático, essa representação para o Controle de Segurança Crítico 1 do CIS (CSC 1):

ID	Política Aprovada	Controle Implementado	Controle Automatizado	Controle Reportado à Direção
1.1	Política Informal (0,25)	Não Implementado (0)	Não Aplicável (Não Contabilizado)	Não Aplicável (Não Contabilizado)
1.2	Política Escrita (0,75)	Implementada em Alguns Sistemas (0,5)	Não Aplicável (Não Contabilizado)	Não Aplicável (Não Contabilizado)
1.3	Política Aprovada (1)	Implementada em Muitos Sistemas (0,75)	Automatizada em Alguns Sistemas (0,5)	Reportada em Muitos Sistemas (0,75)
1.4	Política Parcialmente Escrita (0,5)	Partes da Política Implementadas (0,25)	Automatizada em Alguns Sistemas (0,5)	Não Reportada (0)
1.5	Sem Política (0)	Implementada em Alguns Sistemas (0,5)	Não Automatizado (0)	Não Reportada (0)
Média	$(0,25+0,75+1+0,5+0)/5 = 0,5$	$(0+0,5+0,75+0,25+0,5)/5 = 0,4$	$(0,5+0,5+0)/3 = 0,33$	$(0,75+0+0)/3 = 0,25$

Os 18 controles podem ser monitorados individualmente. Na planilha de cada um deles, há um índice de adequação que monitora as respostas informadas pelo responsável. O índice busca alcançar 100%, que seria o pleno atendimento de cada uma das medidas de segurança em: estar em uma política aprovada, ser um controle implementado em todos os sistemas, estar automatizado e ser reportado à direção:

Índice de Adequação	Média	Aplicação ao CSC 5	%
---------------------	-------	--------------------	---

Medidas de Segurança Adequadas	(Política Aprovada + Controle Implementado + Controle Automatizado + Reportado à Direção)/4	$(0,5+0,4+0,33+0,25)/4 = 0,37$	37%
Medidas de Segurança Não Adequadas	1 –Medidas de Segurança Adequadas	1-0,37	63%

Os níveis de maturidade, por sua vez, utilizam os agrupamentos tratados acima na sua composição, conforme tabela abaixo:

Nível de Maturidade	Descrição	Descrição detalhada
1	Políticas Publicadas	Média dos pesos de todos as Medidas de Segurança analisadas.
2	Controles 1 a 5 Implementados	Média dos pesos de todos as Medidas de Segurança implementadas dos controles de 1 a 5.
3	Todos os Controles Implementados	Média dos pesos de todos as Medidas de Segurança implementadas dos controles de 6 a 18.
4	Todos os Controles Automatizados	Média dos pesos de todos as Medidas de Segurança implementadas dos controles de 1 a 18.
5	Todos os Controles Reportados	Média dos pesos de todos as Medidas de Segurança reportadas à direção dos controles de 1 a 18.

4.3 Gráfico do Dashboard ATT&CK Activity

Nesse gráfico o auditscript faz uma correlação dos controles da documentação CIS-Controls-Version-8 com as táticas MITRE ATT&CK ¹⁴utilizadas como padrão para um ataque cibernético, expondo o cenário atual das ações de defesa cibernética por

¹⁴ A MITRE ATT&CK é uma base de conhecimento acessível globalmente de táticas e técnicas de ataque cibernético

meio da implementação dos Controles CIS e suas Medidas de Segurança.

4.3.1 MITRE ATT&CK

MITRE é uma organização de pesquisa financiada pelo governo americano com sede em Bedford, MA, e McLean, VA. Trabalha com o Instituto Nacional de Padrões e Tecnologia (NIST) para enfrentar o sério e crescente risco que as vulnerabilidades de cibersegurança representam para a prosperidade econômica, segurança pública e segurança nacional.

4.3.2 A estrutura Enterprise ATT&CK

A Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) do MITRE foi criada a partir da necessidade de categorizar sistematicamente o comportamento adversário como parte da realização de exercícios estruturados de emulação adversária dentro do ambiente de pesquisa Fort Meade Experiment¹⁵ da MITRE.

O ATT&CK é uma base de conhecimento e modelo para o comportamento do ataque cibernético, refletindo suas várias fases do ciclo de vida e as plataformas que eles têm como alvo, sendo útil para entender o risco de segurança contra comportamento adverso conhecido, para planejar melhorias de segurança e verificar se as defesas funcionam conforme o esperado.

Existem duas matrizes na estrutura MITRE ATT&CK:

- Enterprise ATT&CK;
- Mobile ATT&CK;

Para esse framework foi utilizada a matriz Enterprise ATT&CK, que é um modelo que explica as ações que um invasor pode tomar para operar dentro de uma rede corporativa. Foca-se principalmente no comportamento pós-exploração. Essa matriz pode ajudar a priorizar a defesa da rede, explicando as táticas, técnicas e

¹⁵ Fort Meade eXperiment (FMX). FMX é um segmento de "laboratório vivo" fortemente monitorado. Acessível em <https://www.mitre.org/careers/working-at-mitre/employee-voices/a-cyber-security-engineer-scores-a-big-win-with-attck>

procedimentos (TTPs) que os atacantes usam uma vez dentro da rede. Seguem as táticas utilizadas:

TÁTICA	DEFINIÇÃO	EXEMPLO
Acesso Inicial	Utilização de técnicas que abrangem vários vetores de entrada para obter uma posição inicial dentro de uma rede.	Spearphishing Link - Envio de e-mail com o uso de links contendo malware, em vez de anexar arquivos maliciosos ao próprio e-mail, assim evitando defesas que inspecionam anexos. Também é possível envolver técnicas de engenharia social, como se passar por uma fonte confiável.
Execução	Utilização de técnicas que resultam na execução de código controlado por invasor em um sistema local ou remoto.	Powershell - É uma poderosa interface de linha de comando interativa e ambiente de script incluído no sistema operacional Windows. O atacante pode usar esse ambiente para realizar uma série de ações, incluindo descoberta de informações e execução de código.
Persistência	Utilização de técnicas para manter o acesso persistente a um sistema.	Scripts de logon - O atacante utiliza scripts que são executados automaticamente na inicialização do sistema ou na inicialização do logon para estabelecer a persistência. Podem ser usados para executar funções administrativas, que muitas vezes executam outros programas ou enviam informações para um servidor de registro interno. Esses scripts podem variar com base no sistema operacional e se aplicados local ou remotamente.
Escalação de privilégios	Utilização de técnicas para obter um nível de privilégio elevado em um sistema ou rede.	Injeção de processos - É um método de execução de código no espaço de endereço de um processo ativo separado, podendo evitar a detecção baseada em processos. Esse código no contexto de outro processo pode permitir o acesso à memória, aos recursos do sistema / rede e, possivelmente, a privilégios elevados.
Evasão de defesa	Utilização de técnicas para evitar a detecção	Preenchimento binário - O atacante pode usar de preenchimento binário para adicionar dados inúteis e alterar a representação do malware no disco. Isso pode ser feito sem afetar a funcionalidade ou o comportamento de

		um binário, mas pode aumentar seu tamanho além do que algumas ferramentas de segurança são capazes de lidar devido às limitações de tamanho de arquivo.
Credencial de acesso	Utilização de técnicas para roubar credenciais, como nomes de login e senhas	Interceptação de MFA - O atacante pode ter como alvo mecanismos de autenticação de múltiplos fatores, para obter acesso a credenciais que podem ser usadas para acessar sistemas, serviços e recursos de rede. O uso desse método de autenticação é recomendado e fornece um nível mais alto de segurança do que login e senha isoladamente, porém as organizações devem estar cientes das técnicas que podem ser usadas para interceptar e contornar esse mecanismo de segurança.
Descoberta	Utilização de técnicas para obter conhecimento sobre o sistema e a rede interna	Sniffing de rede - O atacante pode farejar o tráfego da rede para capturar informações sobre um ambiente, incluindo material de autenticação transmitido pela rede. Pode colocar uma interface de rede em modo promíscuo para acessar passivamente os dados em trânsito pela rede ou usar portas de expansão para capturar uma quantidade maior de dados.
Movimento lateral	Utilização de técnicas para entrar e controlar sistemas remotos em uma rede a partir de um host já comprometido	Passe o hash - é um método de autenticação como usuário sem ter acesso à senha de texto não criptografado. Esse método ignora as etapas de autenticação padrão que exigem uma senha de texto não criptografado, indo diretamente para a parte da autenticação que usa o hash de senha. O atacante captura hashes de senha usando uma técnica de acesso de credencial. Uma vez autenticado, ele pode utilizar para executar ações em sistemas locais ou remotos.

Coleta	Utilização de técnicas para coletar informações relevantes para seguir os objetivos do invasor	Captura de entrada - Durante o uso normal do sistema, os usuários geralmente fornecem credenciais para vários locais diferentes, como páginas / portais de login ou caixas de diálogo do sistema. O atacante utiliza mecanismos de captura de entrada que podem ser transparentes para o usuário (por exemplo, keylogger) ou podem enganar o usuário para que forneça informações sobre o que ele acredita ser um serviço genuíno.
Comando e controle	Utilização de técnicas para se comunicar com os sistemas sob seu controle, muitas vezes disfarçados para se parecer com o tráfego normal	Protocolos da camada de aplicação - O atacante pode se comunicar usando protocolos da camada de aplicação para evitar a detecção / filtragem de rede ao se misturar ao tráfego existente. Os comandos para o sistema remoto e, frequentemente, os resultados desses comandos, serão incorporados ao tráfego de protocolo entre o cliente e o servidor.
Exfiltração	Utilização de técnicas para roubar dados de uma rede	Duplicação de tráfego - O atacante pode aproveitar o espelhamento de tráfego (um recurso nativo em dispositivos de rede utilizado para análise de rede) para automatizar a exfiltração de dados em uma infraestrutura de rede comprometida.
Impacto	Utilização de técnicas para interromper a disponibilidade ou comprometer a integridade ao manipular processos de negócios e operacionais	Dados criptografados - O atacante pode criptografar dados em sistemas de destino ou em um grande número de sistemas em uma rede para interromper a sua disponibilidade. Ele pode tentar tornar os dados armazenados inacessíveis criptografando arquivos ou dados em unidades locais e remotas e reterendo o acesso a uma chave de descryptografia. Em alguns casos, os adversários podem criptografar arquivos de sistema críticos, partições de disco e o MBR. Condicionando a chave de descryptografia a alguma compensação monetária (Ex.: Ransomware).

A planilha é estruturada em 3 (três) níveis de probabilidade, sendo cada nível representando a capacidade de prevenção e detecção de ataques, por meio dos controles do CIS implementados e associados as táticas do MITRE ATT&CK, conforme tabela abaixo:

Probabilidade de Prevenção e Detecção	Percentual de Implementação (%)	
	PREVENÇÃO	DETECÇÃO
Baixo	0 a 25	0 a 25
Moderado	25 a 75	25 a 75
Alto	75 a 100	75 a 100

No anexo I deste documento é apresentado uma tabela com as 12 (doze) táticas mapeadas na planilha da AuditScript, a forma de ataque e os Controles do CIS Associados para Prevenção e Detecção.

4.3.3 Community Defense Model (CDM)

O CIS através de sua comunidade vem mapeando a atividades de ataque com uma abordagem baseada em dados com objetivo de medir a efetividade dos seus controles diante de tais ataques.

Independentemente do tipo de ataque específico, verificou-se que a implementação de medidas de segurança do Grupo de implementação 1 (GI1) defende contra 74% das técnicas de ataques na estrutura MITRE ATT&CK, e a implementação de todas as Medidas de Segurança CIS defende contra 86% dessas técnicas.

Além disso, a CDM correlaciona os cinco ataques de maior incidência com as técnicas apresentadas na matriz ATT&CK, de modo a apresentar uma visão real dos controles do CIS.

Nessa correlação foi possível verificar:

Medidas de Segurança GI 1 CIS	Todas as medidas de
----------------------------------	------------------------

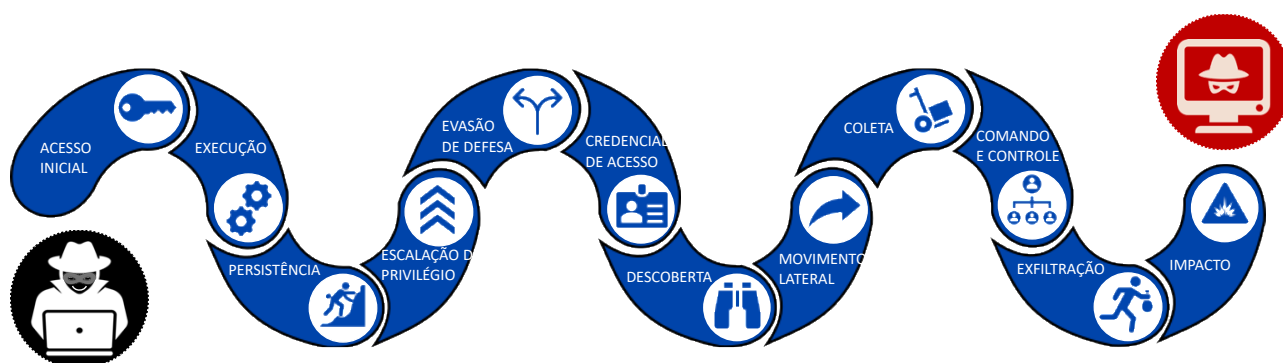
		segurança do CIS
5 principais ataques	GI1 pode se defender contra XX% das técnicas (sub) ATT&CK	As medidas de segurança do CIS podem se defender contra XX% das técnicas(sub) ATT&CK
Malware	77%	94%
Ransomware	78%	92%
Hacking de Aplicativo da Web	86%	98%
Privilégio Interno e Uso Indevido	86%	90%
Instruções direcionadas	83%	95%

4.3.4 Interrupção do ataque

A interrupção do ataque que utiliza como método o conceito em cadeia ou corrente, baseado no processo KILL CHAIN¹⁶, pode inviabilizar todo o ataque planejado.

Para a realização de um ataque cibernético o invasor deve combinar as táticas conforme seu objetivo, nem todo ataque necessariamente deve utilizar as 12 táticas, por exemplo, um ataque DDoS onde não se faz necessária a tática CREDENCIAL DE ACESSO.

Na figura 2 ilustra-se um exemplo em que o atacante precisa percorrer as 12 táticas para atingir seu objetivo conforme o tipo de ataque escolhido.



¹⁶ É um modelo de segurança cibernética criado pela Lockheed Martin que rastreia os estágios de um ataque cibernético, identifica vulnerabilidades e ajuda as equipes de segurança a interromper os ataques em cada estágio da corrente.

Figura 2. Representação gráfica de uma cadeia de ataque cibernético utilizando 12 táticas(elos).

Já na figura 3 o defensor, adequado aos controles CIS a nível satisfatório, preveniu a execução da tática MOVIMENTO LATERAL, dessa forma, interrompendo a execução do ataque.

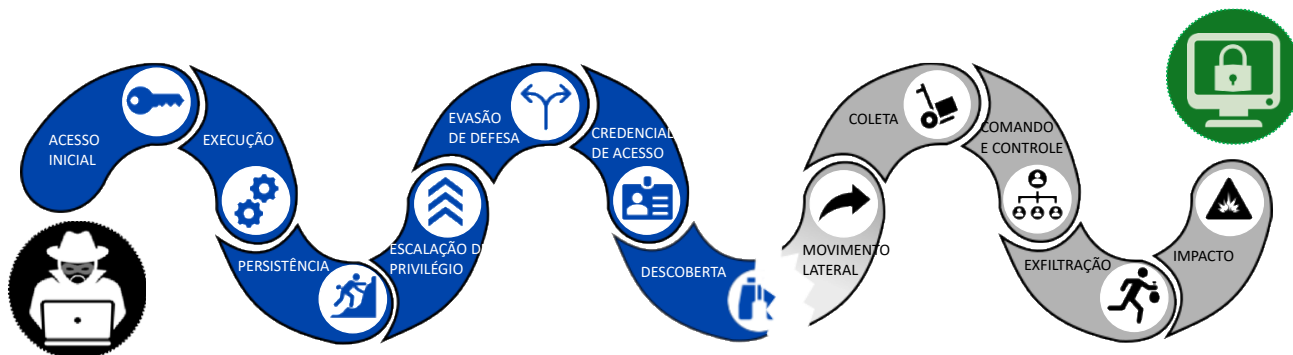


Figura 3. Representação gráfica de uma interrupção da cadeia de ataque cibernético utilizando 12 táticas(elos).

Por fim, é sempre importante reforçar que as instituições que adotem o presente documento são livres para realizarem as adaptações necessárias na planilha e nos requisitos, de maneira a atender a realidade concreta enfrentada em seus trabalhos internos e externos.

Referências Bibliográficas

A Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) - MITRE. Acessível em <https://attack.mitre.org/versions/v10/>.

Center for Internet Security (CIS) Community Defense Model (CDM) v2.0 – CIS Center for Internet Security. Acessível em <https://www.cisecurity.org/blog/cis-introduces-v2-0-of-the-cis-community-defense-model/>.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27001:2013**: Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação - Requisitos. Rio de Janeiro, 2013.

_____. **ABNT NBR ISO/IEC 27002:2013**: Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação. Rio de Janeiro, 2013.

_____. **ABNT NBR ISO/IEC 27005:2019:** Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação. Rio de Janeiro, 2019.

_____. **ABNT NBR ISO/IEC 27701:2019:** Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes. Rio de Janeiro, 2019.

_____. **ABNT NBR ISO/IEC 31000:2018:** Gestão de Riscos — Diretrizes. Rio de Janeiro, 2018.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais.** Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 23 fev. 2021.

AUDITSCRIPTS. CIS Controls Initial Assessment Tool, versão 7.1d. Disponível em: <https://www.auditscripts.com/download/4229/>. Acesso: 28 fev. 2021.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Portaria nº 93, de 26 de setembro de 2019. **Glossário de Segurança da Informação.** Disponível em: <https://www.in.gov.br/en/web/dou/-/portaria-n-93-de-26-de-setembro-de-2019-219115663>. Acesso em: 23 fev. 2021.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. **Instrução Normativa nº 01, de 27 de maio de 2020.** Brasília, DF, GSI/PR, 2020. Disponível em: <http://dsic.planalto.gov.br/assuntos/editoria-c/documentos-pdf-1/instrucao-normativa-no-1-de-27-de-maio-de-2020-1.pdf>. Acesso em: 24 fev. 2021.

CENTER INTERNET SECURITY. **CIS Controls**, versão 7.1. Abril de 2019. Disponível em: <https://learn.cisecurity.org/cis-controls-download>. Acesso em: 28 fev. 2021.

COMITÊ CENTRAL DE GOVERNANÇA DE DADOS - CCGD. **Guia de Boas Práticas LGPD.** Agosto de 2020. Disponível em: <https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-de-boas-praticas-lei-geral-de-protecao-de-dados-lgpd>. Acesso em: 28 fev. 2021.

CYBER SECURITY AGENCY OF SINGAPORE (CSA). **Security-by-Design Framework Versão 1.0.** Singapura, 2017. Disponível em: https://www.csa.gov.sg/-/media/csa/documents/legislation_supplementary_references/security_by_design_framework.pdf. Acesso em: 28 fev. 2021.

DHOLAKIYA, Pratik. **What Is the Cyber Kill Chain and How It Can Protect Against Attacks.** Disponível em: <https://www.computer.org/publications/tech-news/trends/what-is-the-cyber-kill-chain-and-how-it-can-protect-against-attacks>. Acesso em: 10 nov. 2021.

INTERNATIONAL STANDARD. **ISO/IEC 29100:2011:** Information technology — Security techniques — Privacy framework. Genebra, 2011.

_____. **ISO/IEC 29134:2017:** Information technology – Security techniques –

Guidelines for privacy impact assessment. Genebra, 2017.

_____. **ISO/IEC 29151:2017**: Information technology — Security techniques — Code of practice for personally identifiable information protection. Genebra, 2017.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Guia de Aperfeiçoamento da Segurança Cibernética para Infraestrutura Crítica, versão 1.1, 2018. Disponível em: https://www.uschamber.com/sites/default/files/intl_nist_framework_portugese_finalfull_w eb.pdf >. Acesso em: 28 fev. 2021.

_____. **Framework for Improving Critical Infrastructure Cybersecurity**, versão 1.1, 2018. Disponível em: <https://doi.org/10.6028/NIST.CSWP.04162018>. Acesso em: 28 fev. 2021.

_____. **NIST Special Publication 800-53 revisão 5**: Security and Privacy Controls for Information Systems and Organizations. Gaithersburg, 2020.

_____. - Computer Security Resource Center – Glossary. Disponível em: <https://csrc.nist.gov/glossary> . Acesso em: 24 fev. 2021.

SECRETARIA DE GOVERNO DIGITAL. **Guia de Avaliação de Riscos de Segurança e Privacidade**, versão 1.0. Novembro de 2020. Disponível em: <https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-de-avaliacao-de-riscos-de-seguranca-e-privacidade.pdf>. Acesso em: 28 fev. 2021.

SOLVING PROBLEMS FOR A SAFER WORLD. 2021. Disponível em: <https://www.mitre.org/>. Acesso em: 18 nov. 2021.

GUIA DO FRAMEWORK DE SEGURANÇA

ANEXO I

Atividade de Ataque	Como funciona	Controles do CIS Associados para	
		Capacidade de Prevenir	Capacidade de Detectar
ACESSO INICIAL O atacante tenta entrar na sua rede	Consiste em técnicas que usam vários vetores de entrada para obter sua posição inicial dentro de uma rede. As técnicas usadas para se firmar incluem spearphishing direcionado e exploração de pontos fracos em servidores da web voltados para o público. Os pontos de apoio obtidos por meio do acesso inicial podem permitir o acesso continuado, como contas válidas e uso de serviços remotos externos, ou podem ter uso limitado devido à alteração de senhas.	Controle 02 - Inventário e controle de ativos de software	Controle 01 - Inventário e controle de ativos institucionais
		Controle 07 - Gestão contínua de vulnerabilidades	Controle 08 - Gestão de registros de auditoria
		Controle 04 - Configuração segura de ativos institucionais e software	
		Controle 05 - Gestão de contas	
		Controle 09 - Proteções de e-mail e navegador Web	
EXECUÇÃO O atacante tenta executar um código malicioso	Consiste em técnicas que resultam na execução de código controlado pelo atacante em um sistema local ou remoto. As técnicas que executam código malicioso costumam ser combinadas com técnicas de todas as outras táticas para atingir objetivos mais amplos, como explorar uma rede ou roubar dados. Por exemplo, um adversário	Controle 02 - Inventário e controle de ativos de software	Controle 01 - Inventário e controle de ativos institucionais
		Controle 07 - Gestão contínua de vulnerabilidades	Controle 08 - Gestão de registros de auditoria
		Controle 04 - Configuração segura de ativos institucionais e software	

	pode usar uma ferramenta de acesso remoto para executar um script do PowerShell que faz a descoberta de sistema remoto.	Controle 05 - Gestão de contas	
PERSISTÊNCIA O atacante tenta manter sua posição	Consiste em técnicas que o atacante utiliza para manter o acesso aos sistemas durante reinicializações, credenciais alteradas e outras interrupções que poderiam cortar seu acesso. As técnicas usadas para persistência incluem qualquer alteração de acesso, ação ou configuração que os deixe manter sua posição nos sistemas, como substituir ou sequestrar código legítimo ou adicionar código de inicialização.	Controle 02 - Inventário e controle de ativos de software	Controle 01 - Inventário e controle de ativos institucionais
		Controle 07 - Gestão contínua de vulnerabilidades	Controle 08 - Gestão de registros de auditoria
		Controle 04 - Configuração segura de ativos institucionais e software	
		Controle 05 - Gestão de contas	
ESCALAÇÃO DE PRIVILÉGIO O atacante tenta obter permissões de nível superior	Consiste em técnicas que o atacante utiliza para obter permissões de nível superior em um sistema ou rede. O atacante muitas vezes pode entrar e explorar uma rede com acesso sem privilégios, mas exigem permissões elevadas para cumprir seus objetivos. As abordagens comuns são: tirar proveito das fraquezas, configurações incorretas e vulnerabilidades do sistema. Exemplos de escalação de privilégio incluem: • SYSTEM/root;	Controle 02 - Inventário e controle de ativos de software	Controle 01 - Inventário e controle de ativos institucionais
		Controle 07 - Gestão contínua de vulnerabilidades	Controle 08 - Gestão de registros de auditoria
		Controle 04 - Configuração segura de ativos institucionais e software	

	• administrador local; • conta de usuário com acesso de administrador; • contas de usuário com acesso a sistema específico ou função específica. Essas técnicas geralmente se sobrepõem às técnicas de persistência, pois os recursos do sistema operacional que permitem que um atacante persista podem ser executados em um contexto elevado.	Controle 05 - Gestão de contas	
EVASÃO DE DEFESA O atacante tenta evitar sua detecção	Consiste em técnicas que o atacante utiliza para evitar a detecção ao longo de seu comprometimento. As técnicas utilizadas para evasão de defesa incluem desinstalar / desativar software de segurança ou ofuscar / criptografar dados e scripts. O atacante também aproveita e abusa de processos confiáveis para ocultar e disfarçar seu malware. Outras técnicas incluem o benefício adicional de subverter as defesas.	Controle 02 - Inventário e controle de ativos de software	Controle 01 - Inventário e controle de ativos institucionais
		Controle 07 - Gestão contínua de vulnerabilidades	Controle 08 - Gestão de registros de auditoria
		Controle 04 - Configuração segura de ativos institucionais e software	
		Controle 05 - Gestão de contas	
CREDENCIAL DE ACESSO O atacante tenta roubar logins e senhas	Consiste em técnicas para roubar credenciais, como logins e senhas. As técnicas usadas para obter credenciais incluem keylogger ou uso de credencias padrões. O uso de credenciais legítimas pode dar ao atacante acesso aos sistemas, torná-los mais difíceis de detectar e fornecer a	Controle 02 - Inventário e controle de ativos de software	Controle 01 - Inventário e controle de ativos institucionais
		Controle 07 - Gestão contínua de vulnerabilidades	Controle 08 - Gestão de registros de auditoria
		Controle 04 - Configuração segura de ativos institucionais e	

	oportunidade de criar mais contas para ajudar a atingir seus objetivos.	software	
		Controle 05 - Gestão de contas	
		Controle 06 - Gestão do controle de acesso	
DESCOBERTA O atacante tenta descobrir seu ambiente	Consiste em técnicas que o atacante pode utilizar para obter conhecimento sobre o sistema e a rede interna. Essas técnicas ajudam a observar o ambiente e se orientar antes de decidir como agir. Também permitem que o atacante explore o que pode controlar e o que está ao redor de seu ponto de entrada, a fim de descobrir como isso pode beneficiar seu objetivo atual. As ferramentas nativas do sistema operacional costumam ser usadas para esse objetivo de coleta de informações pós-comprometimento.	Controle 02 - Inventário e controle de ativos de software	Controle 01 - Inventário e controle de ativos institucionais
		Controle 07 - Gestão contínua de vulnerabilidades	Controle 08 - Gestão de registros de auditoria
		Controle 04 - Configuração segura de ativos institucionais e software	
		Controle 05 - Gestão de contas	
		Controle 13 - Monitoramento e defesa da rede	
		Controle 14 - Conscientização sobre segurança e treinamento de competências	
		Controle 06 - Gestão do controle de acesso	
MOVIMENTO LATERAL O atacante tenta se mover em seu ambiente	Consiste em técnicas que o atacante utiliza para entrar e controlar sistemas remotos em uma rede. Seguir seu objetivo principal frequentemente requer explorar a rede para encontrar seu alvo e,	Controle 02 - Inventário e controle de ativos de software	Controle 01 - Inventário e controle de ativos institucionais
		Controle 07 - Gestão contínua de vulnerabilidades	Controle 08 - Gestão de registros de auditoria

	subsequentemente, obter acesso a ele. Alcançar seu objetivo geralmente envolve acessar vários sistemas e contas para obter ganhos. O atacante pode instalar suas próprias ferramentas de acesso remoto para realizar o Movimento Lateral ou usar credenciais legítimas com rede nativa e ferramentas de sistema operacional, que podem ser mais furtivas.	Controle 04 - Configuração segura de ativos institucionais e software	
		Controle 05 - Gestão de contas	
		Controle 13 - Monitoramento e defesa da rede	
		Controle 14 - Conscientização sobre segurança e treinamento de competências	
		Controle 06 - Gestão do controle de acesso	
COLEÇÃO O atacante tenta reunir dados relevantes para o seu objetivo	Consiste em técnicas que o atacante pode utilizar para coletar informações e as fontes de informações que são relevantes para o cumprimento dos objetivos do atacante. Frequentemente, o próximo objetivo após a coleta de dados é roubar (exfiltrar) os dados. Fontes de destino comuns incluem vários tipos de unidade, navegadores, áudio, vídeo e e-mail. Os métodos de coleta comuns incluem a captura de capturas de tela e entrada do teclado.	Controle 02 - Inventário e controle de ativos de software	Controle 01 - Inventário e controle de ativos institucionais
		Controle 07 - Gestão contínua de vulnerabilidades	Controle 08 - Gestão de registros de auditoria
		Controle 04 - Configuração segura de ativos institucionais e software	
		Controle 05 - Gestão de contas	
		Controle 12 - Gestão da infraestrutura de rede	
		Controle 13 - Monitoramento e defesa da rede	
		Controle 06 - Gestão do controle de acesso	

COMANDO E CONTROLE O atacante tenta se comunicar com sistemas comprometidos para controlá-los	Comando e controle consiste em técnicas que o atacante pode utilizar para se comunicar com os sistemas sob seu controle dentro da rede comprometida. O atacante geralmente tentam imitar o tráfego normal esperado para evitar a sua detecção. Há muitas maneiras de se estabelecer comando e controle com vários níveis de furtividade, dependendo da estrutura de rede e das defesas da vítima.	Controle 10 - Defesas contra malware	Controle 01 - Inventário e controle de ativos institucionais
		Controle 11 - Recuperação de dados	Controle 08 - Gestão de registros de auditoria
		Controle 12 - Gestão da infraestrutura de rede	Controle 11 - Recuperação de dados
		Controle 13 - Monitoramento e defesa da rede	Controle 13 - Monitoramento e defesa da rede
EXFILTRAÇÃO O atacante tenta roubar dados	Consiste em técnicas que o atacante pode utilizar para roubar dados de sua rede. Depois de coletar os dados, o atacante costuma empacotá-los para evitar a detecção ao removê-los. Isso pode incluir compactação e criptografia. As técnicas para obter dados de uma rede de destino normalmente incluem transferi-los por meio de seu canal de comando e controle ou um canal alternativo e também podem incluir colocar limites de tamanho na transmissão.	Controle 10 - Defesas contra malware	Controle 01 - Inventário e controle de ativos institucionais
		Controle 11 - Recuperação de dados	Controle 08 - Gestão de registros de auditoria
		Controle 12 - Gestão da infraestrutura de rede	Controle 11 - Recuperação de dados
		Controle 13 - Monitoramento e defesa da rede	Controle 13 - Monitoramento e defesa da rede
IMPACTO O atacante tenta manipular, interromper ou destruir sistemas e dados	Consiste em técnicas que o atacante utiliza para interromper a disponibilidade ou comprometer a integridade, manipulando os processos de negócios e operacionais. As técnicas usadas podem	Controle 3 - Proteção de dados	Controle 08 - Gestão de registros de auditoria
		Controle 4 - Configuração segura de ativos institucionais e software	

incluir destruição ou adulteração de dados. Em alguns casos, os processos de negócios podem parecer bons, mas podem ter sido alterados para beneficiar os objetivos do atacante. Essas técnicas podem ser utilizadas para atingir o objetivo final do atacante ou para fornecer cobertura para uma violação de confidencialidade.	Controle 6 - Gestão do controle de acesso	
	Controle 7 - Gestão contínua de vulnerabilidades	
	Controle 11 - Recuperação de dados	
	Controle 12 – Gestão da infraestrutura de rede	
	Controle 18 – Testes de invasão	

ANEXO II Mudanças desta versão

Este anexo tem a finalidade de fornecer uma visão geral das mudanças inseridas nesta versão do Guia de Framework de Segurança em comparação com o documento publicado em Abril de 2021.

Escopo e motivação

Esta versão do Guia de Framework de Segurança teve como escopo e motivação os seguintes pontos:

ESCOPO

- Revisar o documento existente assegurando sua consistência com a versão atual do Controle CIS Versão 8.
- Revisão textual e inclusão de conteúdo e elementos gráficos que pudessem aperfeiçoar o entendimento do framework informado, destacar sua relevância de aplicação no contexto da Administração Pública Federal e adicionar considerações relevantes acerca do dashboard provido pela Auditscript que é parte suplementar ao Guia.

MOTIVAÇÃO

- Assegurar que a estrutura apresentada no Guia estivesse alinhada com a nova versão do Controle CIS e alinhadas com a evolução tecnológica e experiências obtidas a partir da aplicação de tais controles em cenários reais da administração pública brasileira.

Principais Diferenças da Versão CIS 7 e Versão 8

Há diversos elementos pontuais que foram alterados na versão 8 da CIS em comparação com a versão anterior.

A nova versão da CIS apresenta terminologia revisada e agrupamentos diferenciados. Destaca-se a redução da quantidade de medidas de segurança de 20 para 18 a partir da combinação de controles e a criação de uma nova medida chamada Gestão de Provedor de serviço.

Resumo das mudanças

- Medida de segurança 4 (uso controlado de privilégios administrativos) e Medida de segurança 14 (Acesso controlado com base na necessidade de saber) foram combinados na Medida de segurança de gerenciamento de acesso:
- Medida de segurança 05 (configuração segura para hardware e software) e Medida de segurança 11 (configuração segura para dispositivos de rede) foi combinado no controle 4 (uso controlado seguro de ativos institucionais):
- As medidas de segurança 9 (limitações e controle de portas de redes), 12 (defesa de perímetro) e 15 (controle e acesso à rede sem fio) foram excluídas:
- A Medida de segurança 13 proteção de dados foi renumerada para 3:
- Medida de segurança 16 (Monitoramento e controle de credenciais de acesso) foi renomeada para gestão de contas
- Foi criada uma nova medida de segurança de número 15 chamada de gerenciamento de provedor de serviço.

A figura a seguir resume a alteração das referidas medidas:



Community

Figura 2. Mudanças CIS 7 e CIS 8

Defense Model

(CDM)

Para aperfeiçoamento do Guia o CDM foi adicionado para ajudar a responder sobre a eficácia do controle CIS outras questões sobre o valor dos controles com base na ameaça atualmente disponível. O CDM utilizou o framework do MITRE, pois essa metodologia permite medir quais proteções são mais eficazes em geral para a defesa contra os tipos de ataque.

Interrupção do ataque

Foi utilizado o conceito de Kill Chain para representar de forma gráfica a eficácia dos controles do CIS na proteção de um ataque.