Guia do Framework de Segurança

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

Versão 1.0

Brasília, abril de 2021

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 Mario Paes de Andrade

Secretário Especial de Desburocratização, Gestão e Governo Digital

SECRETARIA DE GOVERNO DIGITAL

Luis Felipe Salin Monteiro

Secretário de Governo Digital

DEPARTAMENTO DE GOVERNANÇA DE DADOS E INFORMAÇÕES

Mauro Cesar Sobrinho

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 Revisora

Marcelo de Lima

Histórico de Versões

Data	Versão	Descrição	Autor
12/04/2021	1.0	Primeira versão do Guia do Framework de Segurança.	Equipe Técnica de Elaboração

SUMÁRIO

AVISO PRELIMINAR E AGRADECIMENTOS

O presente guia buscar 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 pode 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 *AuditScripts*[2] 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, 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 operacionais[4] elaborados pela Secretaria de Governo Digital (SGD), da Secretaria Especial de Desburocratização, Gestão e Governo Digital do

[1] https://www.cisecurity.org/
[2] https://www.auditscripts.com/
[3] https://www.nist.gov/cyberframework/framework
[4] https://www.gov.br/governodigital/pt-br/governanca-de-dados/guias-operacionais-para-adequacao-a-lgpd

Ministério da Economia para fomentar a adequação à proteção dos dados pessoais[5][6][7]. Um desses documentos operacionais, o Guia de Avaliação de Riscos de Segurança e Privacidade[8], pode 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 tratados[9] por ele. A avaliação descrita no Guia de Avaliação de Riscos de Segurança e Privacidade é realizada por uma ferramenta de acesso aberto ao público[10].

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 20 Controles de Segurança elaborados pelo CIS.

Para tanto, o Guia é inspirado nos documentos: *CIS Control*, versão 7.1, AuditScripts-CIS-Controls-Initial-Assessment-Tool, versão 7.1d e *Framework for Improving Critical Infrastructure Cybersecurity*, versão 1.1. O Guia não substitui a leitura dos documentos originais na busca por informações complementares.

O documento (ferramenta) AuditScripts-CIS-Controls-Initial-Assessment-Tool oferece a possibilidade de acompanhar a implementação dos 20 controles do CIS por meio da alimentação de informações numa planilha com gráficos que permitem identificar o estágio atual da instituição. A 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 funcionamento do documento a partir dessas adaptações.

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 20 Controles do CIS. O último capítulo versa sobre o funcionamento da ferramenta de acompanhamento da implementação dos 20 controles do CIS.

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

---

[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] 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] https://pesquisa.sisp.gov.br/index.php/468289?lang=pt-BR

Ressalta-se que a instituição é livre para adequar todas as proposições deste guia a sua realidade. A abordagem do Guia 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 instituição a concentrar seus esforços com base nos recursos de que dispõe, integrando-os a qualquer processo de gestão de risco pré-existente.

No mesmo sentido, deve ser recordado 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 sobre a maturidade de seus trabalhos de segurança da informação e de proteção de dados e ao 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 subcontroles específicos que devem ser atendidos e são cumulativos 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). Os subcontroles selecionados para o Grupo de Implementação 1 podem ser implementados, ou devem ser implementáveis, com experiência limitada em segurança cibernética e são destinados a impedir ataques gerais não direcionados.

Grupo de Implementação 2:

É representado por uma instituição com profissionais dedicado 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 cidadãos**[11], o que incluí **dados pessoais**[12], 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. Os subcontroles selecionados para o Grupo de Implementação 2 ajudam as equipes

[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.

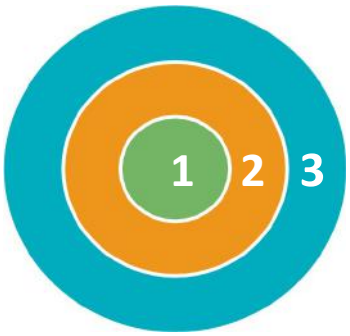
[12] Lei nº 13.709/2018, art. 5º, inciso I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável.

de segurança a lidar com o aumento da complexidade operacional. Alguns subcontroles 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. Os subcontroles selecionados 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 subcontroles de perfil mais avançado sejam implementados na instituição. A tabela abaixo resume a visão dos grupos de implementação:



Grupo de Implementação (GI)	Total de subcontroles (%)	Definição
1	43 (25%)	Subcontroles para pequenas instituições em que o tratamento dos dados no ambiente interno é pouco sensível. Lembrar que as medidas do GI 1 são cumulativas nos GI 2 e GI 3.
2	140 (82%)	Subcontroles focados em ajudar os times de segurança a gerir dados sensíveis e pessoais de cidadãos e instituições. Inclui as medidas do GI 1.
3	171 (100%)	Subcontroles reduzem o impacto de ataques zero-day e ataques mais sofisticados. Inclui as medidas do GI 1 e do GI 2.

Figura 1. Adaptado do CIS Control v7.1

2 – NIST

A ferramenta criada pela instituição AuditScripts (e adaptada para este documento) enquadra os subcontroles do CIS dentro de quatro das cinco funções da Estrutura Básica definidas na publicação **Guia de Aperfeiçoamento da Segurança Cibernética para Infraestrutura Crítica**[13] do NIST. As quatro funções são: identificar, proteger, detectar e responder.

Para este documento, um dos objetivos da inclusão das quatro funções é facilitar a classificação das ações (implementação dos subcontroles) 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 os subcontroles às ações dos seus planos de tratamento de riscos.

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

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.

[13] https://www.uschamber.com/sites/default/files/intl_nist_framework_portugese_finalfull_web.pdf

- 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 20 controles do CIS, seus respectivos subcontroles e a indicação do grupo de implementação correlato.

CIS Controle 1: Inventário e Controle de Ativos de Hardware

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.

CIS Controle 1: Inventário e Controle de Ativos de Hardware

Subcontrole ID	NIST CSF	Linha de Base	Detalhamento do Controle de Segurança Crítico	Grupo de Implementação
1.1	Identificar	Ferramenta de Descoberta Ativa	Utilizar uma ferramenta de descoberta ativa para identificar dispositivos conectados à rede da instituição e atualizar o inventário de ativos de hardware.	2
1.2	Identificar	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
1.3	Identificar	Usar o Registro de Log do DHCP para Atualizar o Inventários de Ativos	Utilizar o registro (logs) do *Dynamic Host Configuration Protocol* (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
1.4	Identificar	Manter o Inventário de Ativos Detalhado	Manter de forma precisa e atualizada o inventário de todos os ativos tecnológicos com potencial para armazenar e processar informações. Este inventário deve incluir todos os ativos, conectados à rede da instituição ou não.	1
1.5	Identificar	Manter as Informações do Inventário de Ativos	Garantir que o inventário de ativos registre o endereço de rede, o endereço de hardware, o nome do equipamento, o dono do ativo, e o departamento em que cada ativo está lotado, bem como se ele foi aprovado para conectar à rede.	2
1.6	Responder	Retirar Ativos Não Autorizados	Garantir que ativos não autorizados sejam removidos da rede, colocados em quarentena ou que o inventário seja atualizado em tempo hábil.	1
1.7	Proteger	Implantar Controle de Acesso em Nível de Porta	Utilizar o controle de acesso de nível de porta, seguindo os padrões 802.1x, para controlar quais dispositivos podem ser autenticados na rede. O sistema de autenticação deve ser vinculado aos dados do inventário de ativos de hardware para garantir que apenas dispositivos autorizados estejam conectados à rede.	2
1.8	Proteger	Utilizar Certificado Cliente para Autenticar Ativos de Hardware	Utilizar certificados cliente (de máquina) para autenticar ativos de hardware que se conectam à rede 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.

CIS Controle 2: Inventário e Controle de Ativos de Software

Subcontrole ID	NIST CSF	Linha de Base	Detalhamento do Controle de Segurança Crítico	Grupo de Implementação
2.1	Identificar	Manter um Inventário de Software Autorizado	Manter uma lista atualizada de todos os softwares autorizados que sejam necessários à instituição independente propósito.	1
2.2	Identificar	Garantir que o Software é Suportado pelo Fabricante	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.	1
2.3	Identificar	Utilizar Ferramentas de Inventário de Software	Utilizar ferramentas de inventário de software em toda a instituição para automatizar a documentação de todos os softwares que componham sistemas de negócio.	2
2.4	Identificar	Trilha de Informações do Inventário de Software	O sistema de inventário de software deve registrar o nome, versão, fabricante e data de instalação de todos os softwares, incluindo sistemas operacionais autorizados pela organização.	2
2.5	Identificar	Integração entre Inventário de Software e Hardware	O sistema de inventário de software deve ser vinculado ao inventário de ativos de hardware para que todos os dispositivos e softwares associados sejam rastreados a partir de um único local.	3
2.6	Identificar	Retirar Software Não Aprovado	Garantir que o software não autorizado seja removido e que o inventário seja atualizado em tempo hábil.	1
2.7	Proteger	Utilizar Aplicações de Whitelisting	Utilizar tecnologia de "whitelisting" em todos os ativos para garantir que apenas software autorizado seja executado, e que todos os softwares não autorizados tenham sua execução bloqueada.	3
2.8	Proteger	Utilizar Aplicações de Whitelisting de Bibliotecas	O software de "whitelisting" deve garantir que apenas bibliotecas autorizadas (tais como *.dll, *.ocx, *.so, etc) tenham permissão para serem carregadas nos processos em execução.	3
2.9	Proteger	Utilizar Aplicações de Whitelisting de Scripts	O software de "whitelisting" deve garantir que apenas scripts autorizados e assinados digitalmente (tais como *.ps1, *.py, macros etc.) tenham permissão para serem executados.	3
2.10	Proteger	Segregar as Aplicações de Alto Risco Fisicamente ou Logicamente	Utilizar a segregação de sistemas logicamente ou fisicamente para isolar ou executar software necessário para operações de negócios, mas que incorrem em alto risco para a organização.	3

CIS Controle 3: Gestão Contínua de Vulnerabilidades

Adquira, avalie e execute ações continuamente em novas informações a fim de identificar vulnerabilidades, corrigir e minimizar a janela de oportunidade para os invasores.

CIS Controle 3: Gestão Contínua de Vulnerabilidades

Subcontrole ID	NIST CSF	Linha de Base	Detalhamento do Controle de Segurança Crítico	Grupo de Implementação
3.1	Detectar	Executar Ferramenta de Varredura de Vulnerabilidades	Utilizar uma ferramenta de varredura de vulnerabilidades atualizada e compatível com o *Security Content Automation Protocol* (SCAP) para varrer automaticamente todos os ativos conectados à rede com frequência semanal ou inferior, para identificar todas as vulnerabilidades potenciais nos ativos da instituição.	2
3.2	Detectar	Executar Ferramenta de Varredura de Vulnerabilidades Autenticada	Executar varredura de vulnerabilidade autenticada com agentes executados localmente em cada sistema ou com *scanners* remotos configurados com direitos elevados no sistema que está sendo testado.	2
3.3	Detectar	Utilizar Contas dedicadas para Varredura Autenticada	Utilizar uma conta dedicada para verificações de vulnerabilidade autenticadas, que não deve ser usada para nenhuma outra atividade administrativa e deve ser vinculada a máquinas específicas em endereços IP específicos.	2
3.4	Proteger	Implantar Ferramenta Automatizada de Gestão de Patches de Sistemas Operacionais	Implantar ferramentas de atualização de software automatizadas para garantir que os sistemas operacionais estejam executando as atualizações de segurança mais recentes fornecidas pelo fornecedor do software.	1
3.5	Proteger	Implantar Ferramenta Automatizada de Gestão de Patches de Softwares em Geral	Implantar ferramentas de atualização de software automatizadas para garantir que o software de terceiros em todos os equipamentos esteja executando as atualizações de segurança mais recentes fornecidas pelo fornecedor do software.	1
3.6	Responder	Comparar Varreduras de Vulnerabilidades	Comparar regularmente os resultados de varreduras de vulnerabilidades realizadas periodicamente para verificar se as vulnerabilidades foram corrigidas e em tempo hábil.	2
3.7	Responder	Utilizar um Processo de Classificação de Riscos	Utilizar um processo de classificação de risco para priorizar a correção das vulnerabilidades descobertas.	2

CIS Controle 4: Uso Controlado de Privilégios Administrativos

Utilize processos e ferramentas para rastrear / controlar / prevenir / corrigir o uso, atribuição e configuração de privilégios administrativos em computadores, redes e aplicativos.

CIS Controle 4: Uso Controlado de Privilégios Administrativos

Subcontrole ID	NIST CSF	Linha de Base	Detalhamento do Controle de Segurança Crítico	Grupo de Implementação
4.1	Detectar	Manter um Inventário das Contas Administrativas	Utilizar ferramentas automatizadas para inventariar todas as contas administrativas, incluindo contas locais e de domínio, para garantir que apenas indivíduos autorizados tenham privilégios elevados.	2
4.2	Proteger	Alterar Senhas Padrões	Antes de ativar qualquer novo ativo, altere todas as senhas padrão para ter valores consistentes com contas de nível administrativo.	1
4.3	Proteger	Utilizar Contas Administrativas Dedicadas	Garantir que todos os usuários com contas administrativas utilizem uma conta secundária para atividades de privilégio elevado. Esta conta deve ser utilizada somente para atividades administrativas e não para navegação na internet, correio eletrônico ou atividades similares.	1
4.4	Proteger	Utilizar Senhas Únicas	Onde a autenticação multifator não é suportada (como administrador local, root ou contas de serviço), as contas utilizarão senhas que sejam únicas para o sistema em questão.	2
4.5	Proteger	Utilizar Autenticação Multifator para Todas as Contas Administrativas	Utilizar autenticação multifator e canais criptografados para todos os acessos de contas administrativas.	2
4.6	Proteger	Utilizar Máquinas Dedicadas para Atividades Administrativas	Garantir que os administradores usem uma máquina dedicada para todas as tarefas administrativas ou tarefas que requerem acesso administrativo. Esta máquina deve ser segmentada da rede primária da organização e não deve ter o acesso à Internet permitido. Esta máquina não deve ser usada para ler e-mails, redigir documentos ou navegar na Internet.	2
4.7	Proteger	Limitar o Acesso de Ferramentas de Script	Limite o acesso às ferramentas de script (como Microsoft® PowerShell e Python) apenas para usuários administrativos ou de desenvolvimento com a necessidade de acessar esses recursos.	2
4.8	Detectar	Alertar e Registrar Log em Mudanças no Grupo de Membros Administrativo	Configurar os sistemas para gerar uma entrada de registro (log) e alertar quando uma conta for adicionada ou removida de qualquer grupo de privilégios administrativos.	2
4.9	Detectar	Alertar e Registrar Log em Acessos Malsucedidos de Login Administrativo	Configurar os sistemas para gerar uma entrada de registro (log) e alertar sobre logins malsucedidos em uma conta administrativa.	2

CIS Controle 5: Configuração Segura para Hardware e Software

Estabeleça, implemente e gerencie ativamente (rastreie, relate, corrija) a configuração de segurança de dispositivos móveis, laptops, servidores e estações de trabalho utilizando um gerenciamento de configuração rigoroso e processo de controle de alterações para evitar que invasores explorem serviços e configurações vulneráveis.

CIS Controle 5: Configuração Segura para Hardware e Software

Subcontrole ID	NIST CSF	Linha de Base	Detalhamento do Controle de Segurança Crítico	Grupo de Implementação
5.1	Proteger	Estabelecer Configurações Seguras	Manter padrões de configuração de segurança (*baselines*, *hardening*) documentados para todos os sistemas operacionais e softwares autorizados.	1
5.2	Proteger	Manter Imagens Seguras	Manter imagens ou modelos seguros e atualizados para todos os sistemas da instituição com base nos padrões de configuração aprovados da instituição. Qualquer implantação de novo sistema ou sistema existente que seja comprometido deve ter sua imagem criada usando uma dessas imagens ou modelos.	2
5.3	Proteger	Armazenar Imagens Modelos Seguramente	Armazenar as imagens e modelos em servidores configurados de forma segura, validados com ferramentas de monitoramento de integridade, para garantir que apenas as alterações autorizadas nas imagens sejam possíveis.	2
5.4	Proteger	Implantar Ferramenta de Gerenciamento de Configuração	Implantar ferramentas de gerência de configuração de sistemas que automaticamente imponham e reapliquem opções de configuração sobre os sistemas em intervalos regulares agendados.	2
5.5	Detectar	Implementar Sistema de Monitoramento de Configuração	Utilizar um sistema de monitoramento de configuração compatível com o *Security Content Automation Protocol* (SCAP) para verificar todos os elementos de configuração de segurança, catalogar exceções aprovadas e alertar quando ocorrerem alterações não autorizadas.	2

CIS Controle 6: Manutenção, Monitoramento e Análise de Logs de Auditoria

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

CIS Controle 6: Manutenção, Monitoramento e Análise de Logs de Auditoria

Subcontrole ID	NIST CSF	Linha de Base	Detalhamento do Controle de Segurança Crítico	Grupo de Implementação
6.1	Detectar	Utilizar Três Fontes de Sincronização de Tempo	Utilizar pelo menos três fontes de tempo sincronizadas das quais todos os servidores e dispositivos de rede recuperem informações de tempo regularmente para que os "timestamps" dos logs (horários e dadas no registro de log) sejam consistentes.	2

6.2	Detectar	Ativar Registro de Log de Auditoria	Garantir que o registro de log local foi habilitado em todos os sistemas e dispositivos de rede.	1
6.3	Detectar	Habilitar Registro de Log Detalhado	Habilitar o registro de log do sistema para incluir informações detalhadas como fonte de evento, data, usuário, carimbo de data / hora, endereços de origem, endereços de destino e outros elementos úteis.	2
6.4	Detectar	Garantir Armazenamento Adequado dos Registros de Log	Garantir que todos os sistemas que armazenam registros de log tenham espaço de armazenamento adequado para os logs gerados.	2
6.5	Detectar	Gerenciamento Central do Registro de Log	Garantir que os logs apropriados estão sendo agregados a um sistema central de gerenciamento de log para análise e revisão.	2
6.6	Detectar	Implantar SIEM ou Ferramenta Analítica de Registro de Log	Implantar *Security Information and Event Management* (SIEM) ou ferramenta analítica de logs para correlação e análise de logs.	2
6.7	Detectar	Analisar Regularmente os Registros de Log	Analisar regularmente os registros de log para identificar anomalias ou eventos anormais.	2
6.8	Detectar	Realizar Ajustes no SIEM Regularmente	Ajustar regularmente o sistema SIEM para identificar melhor os eventos acionáveis e diminuir o ruído do evento.	2

CIS Controle 7: Proteções para e-mail e Navegadores Web

Minimize a superfície de ataque e as oportunidades para os invasores manipularem o comportamento humano por meio de sua interação com navegadores web e sistemas de e-mail.

CIS Controle 7: Proteções para e-mail e Navegadores Web

Subcontrole ID	NIST CSF	Linha de Base	Detalhamento do Controle de Segurança Crítico	Grupo de Implementação
7.1	Proteger	Utilizar Softwares Suportados pelo Fabricante	Garantir que apenas navegadores web e clientes de e-mail totalmente suportados tenham permissão para executar na instituição, de preferência usando apenas a versão mais recente fornecida pelo fornecedor.	1
7.2	Proteger	Remover Software Não Autorizados	Desinstalar ou desativar qualquer navegador não autorizado ou *plug-ins* de cliente de e-mail ou aplicativos complementares.	2
7.3	Proteger	Limitar o Uso de Linguagens de Scripts em Navegadores Web e Clientes de E-mail	Garantir que apenas as linguagens de *script* autorizadas possam ser executadas em todos os navegadores web e clientes de e-mail.	2

7.4	Proteger	Manter Filtros de URL Baseados em Rede	Aplicar filtros de URL baseados em rede que limitam a capacidade de um sistema de se conectar a sites não aprovados pela instituição. Esta filtragem deve ser aplicada a cada um dos sistemas da instituição, estejam eles fisicamente nas instalações da instituição ou não.	**2**
7.5	Proteger	Subscrever Serviços de Categorização de URLs	Subscrever serviços de categorização de URLs de forma a garantir que o filtro esteja atualizado com base nas mais recentes definições de categorias de sites disponíveis. Sites não categorizados devem ser bloqueados por padrão.	**2**
7.6	Detectar	Registrar Todas as Solicitações a URL	Realizar o registro de log de todas as solicitações de URL de cada um dos sistemas da instituição, seja no local ou em um dispositivo móvel, a fim de identificar atividades potencialmente maliciosas e ajudar os operadores de incidentes a identificar sistemas potencialmente comprometidos.	**2**
7.7	Proteger	Utilizar Serviços de Filtragem de DNS	Utilizar serviços de filtragem de DNS para auxiliar no bloqueio de acessos a domínios maliciosos.	**1**
7.8	Proteger	Implementar DMARC, SPF e DKIM	De forma a diminuir a possibilidade do recebimento de e-mails forjados ou modificados recebidos de domínios válidos, implementar políticas e verificações com base no padrão "*Domain-based Message Authentication, Reporting and Conformance* (DMARC)", iniciando pela implementação dos padrões *Sender Policy Framework* (SPF) e *DomainKeys Identified Mail* (DKIM).	**2**
7.9	Proteger	Bloquear Tipos de Arquivos Desnecessários	Bloquear todos os anexos de e-mail que entram no gateway de correio eletrônico da organização se os tipos de arquivo forem desnecessários para os negócios da instituição.	**2**
7.10	Proteger	Analisar Anexos de E-mail	Utilizar "sandboxing" para analisar e bloquear anexos em e-mails de entrada que apresentem comportamento malicioso.	**3**

CIS Controle 8: Defesas contra Malware

Controle a instalação, disseminação e execução de código malicioso em vários pontos da empresa, enquanto otimiza o uso da automação para permitir a atualização rápida da defesa, coleta de dados e ação corretiva.

CIS Controle 8: Defesas contra Malware

Subcontrole ID	NIST CSF	Linha de Base	Detalhamento do Controle de Segurança Crítico	Grupo de Implementação
8.1	Proteger	Utilizar Software Anti-Malware Gerenciado Centralmente	Utilizar software anti-malware gerenciado centralmente para monitorar e defender continuamente cada uma das estações de trabalho e servidores da instituição.	**2**
8.2	Proteger	Manter Assinaturas Anti-Malware Atualizadas	Garantir que o software anti-malware da instituição atualize seu mecanismo de varredura e banco de dados de assinatura regularmente.	**1**

8.3	Proteger	Habilitar Funcionalidades Anti-Exploits	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**
8.4	Detectar	Varrer Mídias Removíveis com Anti-Malware	Configurar os dispositivos para que eles conduzam automaticamente uma varredura anti-malware em mídia removível quando inseridas ou conectadas ao equipamento.	**1**
8.5	Proteger	Não Executar Conteúdos Automaticamente de Mídias Removíveis	Configurar os dispositivos para não executarem conteúdo automaticamente a partir de mídia removível.	**1**
8.6	Detectar	Centralizar os Registros de Log Anti-Malware	Enviar todos os eventos de detecção de malware para ferramentas de administração de anti-malware e servidores de log de eventos para análise e alerta.	**2**
8.7	Detectar	Habilitar Registro de Log em Consultas DNS	Habilitar o registro de log de consulta do servidor DNS (*Domain Name System*) para detectar pesquisas de nomes de host para domínios maliciosos conhecidos.	**2**
8.8	Detectar	Habilitar Registro de Log sobre Ferramentas de Linha de Comando	Habilitar o log de auditoria sobre ferramentas de linha de comando, tais como Microsoft Powershell e Bash.	**2**

CIS Controle 9: Limitação e Controle de Portas de Rede

Gerenciar (rastrear / controlar / corrigir) a utilização operacional contínua de portas, protocolos e serviços em dispositivos em rede, a fim de minimizar as janelas de vulnerabilidade disponíveis para os invasores.

CIS Controle 9: Limitação e Controle de Portas de Rede

Subcontrole ID	NIST CSF	Linha de Base	Detalhamento do Controle de Segurança Crítico	Grupo de Implementação
9.1	Identificar	Registrar e Integrar no Inventários de Hardware Portas, Serviços e Protocolos	Associar portas ativas, serviços e protocolos aos ativos no inventário de hardware.	**2**
9.2	Proteger	Permitir apenas Portas de Rede, Protocolos e Serviços Aprovados	Garantir que somente portas de rede, protocolos e serviços com requisitos de negócio validados estejam em execução em cada sistema.	**2**
9.3	Detectar	Varrer Portas Regularmente	Realizar varreduras de portas automatizadas regularmente em todos os sistemas e alertar se portas não autorizadas forem detectadas em um sistema.	**2**
9.4	Proteger	Implantar Ferramentas de Filtragem de Portas	Aplicar firewalls locais ou ferramentas de filtragem de portas em cada equipamento, contendo uma regra padrão que descarte todo o tráfego, exceto aqueles serviços e portas que sejam explicitamente permitidos.	**1**

9.5	Proteger	Implementar Firewall de Aplicação	Colocar firewalls de aplicação na frente de quaisquer servidores críticos para verificar e validar o tráfego que vai para o servidor. Qualquer tráfego não autorizado deve ser bloqueado e registrado em log.	**3**

CIS Controle 10: Capacidade de Recuperação de Dados

Utilize processos e ferramentas adequados para fazer o backup das informações críticas com uma metodologia comprovada para recuperação oportuna delas.

CIS Controle 10: Capacidade de Recuperação de Dados

Subcontrole ID	NIST CSF	Linha de Base	Detalhamento do Controle de Segurança Crítico	Grupo de Implementação
10.1	Proteger	Realizar Backups Automatizados e Regularmente	Garantir que todos os dados dos sistemas tenham cópias de segurança (*backups*) realizados automaticamente e de forma regular.	**1**
10.2	Proteger	Realizar Backups Completos	Garantir que todos os principais sistemas da instituição tenham cópias de segurança (*backup*) como um sistema completo, por meio de processos como o de geração de imagens, para permitir a recuperação rápida de um sistema inteiro.	**1**
10.3	Proteger	Testar Backups	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**
10.4	Proteger	Proteger Backups	Garantir que os *backups* 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.	**1**
10.5	Proteger	Garantir a Existência de Backups Offline	Garantir que todos os backups tenham pelo menos um destino de backup *offline* (ou seja, não acessível por meio de uma conexão de rede).	**1**

CIS Controle 11: Configurações Seguras para Dispositivos de Rede

Estabeleça, implemente e gerencie ativamente (rastreie, reporte, corrija) a configuração de segurança de dispositivos de infraestrutura de rede utilizando um gerenciamento de configuração rigoroso e processo de controle de alterações para evitar que invasores explorem serviços e configurações vulneráveis.

CIS Controle 11: Configurações Seguras para Dispositivos de Rede

Subcontrole ID	NIST CSF	Linha de Base	Detalhamento do Controle de Segurança Crítico	Grupo de Implementação
11.1	Proteger	Manter Configurações de Segurança Padrão	Manter padrões de configuração de segurança documentados para todos os dispositivos de rede autorizados.	**2**

11.2	Proteger	Documentar Regras de Tráfego	Todas as regras de configuração que permitam o fluxo de dados através dos dispositivos de rede devem ser documentadas em um sistema de gerência de configuração contendo um requisito de negócio específico para cada regra, o nome de um indivíduo específico responsável por cada requisito, e um prazo de validade para cada requisito.	**2**
11.3	Detectar	Verificar se Configurações Padrões Foram Alteradas	Comparar todas as configurações de dispositivos de rede com as configurações de segurança aprovadas definidas para cada dispositivo de rede em uso e alertar quando quaisquer diferenças forem descobertas.	**2**
11.4	Proteger	Manter Dispositivos Atualizados	Instalar a versão estável mais recente de todas as atualizações relacionadas à segurança em todos os dispositivos de rede.	**1**
11.5	Proteger	Implantar Multifator e Sessões Criptografadas	Gerenciar todos os dispositivos de rede usando autenticação multifator e sessões criptografadas.	**2**
11.6	Proteger	Utilizar Máquinas Dedicadas para Atividades Administrativas	Garantir que os administradores de rede usem uma máquina dedicada para todas as tarefas administrativas ou tarefas que requerem acesso elevado. Esta máquina deve ser segmentada da rede primária da organização e não deve ter acesso à Internet permitida. Esta máquina não deve ser usada para ler e-mails, redigir documentos ou navegar na Internet.	**2**
11.7	Proteger	Gerenciar Infraestrutura de Rede por Redes Dedicadas	Gerenciar a infraestrutura de rede a partir de conexões de rede segregadas da utilização da rede para os negócios da instituição, contando com VLANs distintas ou, preferencialmente, com conectividade física distinta para as sessões de administração dos dispositivos de rede.	**2**

CIS Controle 12: Defesa de Perímetro

Detecte / previna / corrija o fluxo de transferência de informações entre redes de diferentes níveis de confiança.

CIS Controle 12: Defesa de Perímetro

Subcontrole ID	NIST CSF	Linha de Base	Detalhamento do Controle de Segurança Crítico	Grupo de Implementação
12.1	Identificar	Manter um Inventários das Fronteiras da Rede	Manter um inventário atualizado de todas as fronteiras da rede da instituição.	**1**
12.2	Detectar	Varrer em Busca de Conexões Não Autorizadas nas Fronteiras	Realizar varreduras regulares a partir de origem externa a cada fronteira para tentar detectar conexões não autorizadas que sejam acessíveis através da fronteira.	**1**
12.3	Proteger	Negar Comunicações com Endereços IP Maliciosos	Negar comunicações com endereços IP na Internet que sejam reconhecidamente maliciosos ou que não sejam utilizados, e limitar o acesso somente a intervalos de endereços confiáveis e necessários em cada uma das fronteiras da rede da instituição.	**3**
12.4	Proteger	Negar Comunicações com Porta Não Autorizadas	Impedir comunicações com portas TCP ou UDP ou tráfego de aplicação não autorizado, de forma a garantir que apenas protocolos autorizados tenham seu tráfego permitido em ambos os sentidos através de cada uma das fronteiras da rede da instituição.	**2**

12.5	Detectar	Configurar Sistemas de Monitoramento para Registrar Pacotes	Configurar os sistemas de monitoramento para gravarem pacotes de rede que atravessem cada uma das fronteiras da rede da instituição.	**3**
12.6	Detectar	Implantar IDS	Implantar sensores de Sistemas de Detecção de Intrusão (IDS) baseados em rede para identificar mecanismos não usuais de ataque e detectar comprometimento dos sistemas em cada uma das fronteiras da rede da instituição.	**1**
12.7	Detectar	Implantar IPS	Implantar Sistemas de Prevenção de Intrusão (IPS) para bloquear tráfego de rede malicioso em cada uma das fronteiras da rede da instituição.	**2**
12.8	Detectar	Implantar Netflow na Fronteira	Habilitar a coleta de Netflow e registros de log em cada um dos dispositivos existentes nas fronteiras da rede.	**3**
12.9	Proteger	Implantar Proxy na Camada de Aplicação	Garantir que todo o tráfego de entrada ou de saída entre a rede institucional e a Internet passe por um proxy de camada de aplicação que exija autenticação, de forma a filtrar conexões não autorizadas.	**3**
12.10	Detectar	Decifrar Tráfego no Proxy	Decifrar no proxy de borda todo o tráfego criptografado antes de analisar o conteúdo. Entretanto, a instituição pode utilizar "whitelists" de sites cujo acesso possa ser realizado sem que o tráfego seja decifrado.	**1**
12.11	Proteger	Exigir ao Acessos Remotos Multifator de Autenticação	Exigir que todos os acessos remotos à rede da instituição criptografem os dados em trânsito e utilizem autenticação multifator.	**1**
12.12	Proteger	Gerenciar Todos os Logins Remotos à Rede Interna	Realizar varreduras, antes do acesso, em todos os equipamentos que realizem acesso remoto à rede da instituição para garantir que cada uma das políticas de segurança da instituição tenham sido aplicadas da mesma forma que nos dispositivos da rede local.	**3**

CIS Controle 13: 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.

CIS Controle 13: Proteção de Dados

Subcontrole ID	NIST CSF	Linha de Base	Detalhamento do Controle de Segurança Crítico	Grupo de Implementação
13.1	Identificar	Manter Inventário de Informações Sensíveis	Manter um inventário de todas as informações sensíveis (o que incluí dados pessoais) armazenadas, processadas ou transmitidas pelos sistemas de tecnologia da instituição, incluindo aquelas localizados no local ou em um provedor de serviços remoto.	**1**
13.2	Proteger	Remover Dados Sensíveis	Remover da rede dados sensíveis ou sistemas com dados sensíveis (incluindo dados pessoais) não acessados regularmente pela instituição. Esses sistemas devem ser usados apenas como sistemas autônomos (desconectados da rede) pela unidade de negócios que precisa ocasionalmente usar o sistema ou completamente virtualizados e desligados até que seja necessário.	**1**

13.3	Identificar	Monitorar e Bloquear Tráfego de Rede Não Autorizado	Implantar uma ferramenta automatizada nos perímetros da rede para monitorar a transferência não autorizada de informações sensíveis (incluindo dados pessoais) e bloquear essas transferências, alertando os profissionais de segurança da informação.	**3**
13.4	Proteger	Permitir apenas Acesso Autorizado	Permitir acesso apenas a soluções autorizadas de armazenamento de arquivos e provedores de e-mail em nuvem.	**2**
13.5	Detectar	Monitorar e Detectar uso Não Autorizado de Criptografia	Monitorar todo o tráfego que sai da instituição e detectar qualquer uso não autorizado de criptografia.	**3**
13.6	Proteger	Criptografar Dados em Dispositivos Móveis	Utilizar mecanismos criptográficos aprovados para proteger os dados da instituição armazenados em todos os dispositivos móveis.	**1**
13.7	Identificar	Gerenciar Dispositivos USB	Caso seja necessária a utilização de dispositivos de armazenamento USB, deve ser utilizada solução corporativa capaz de configurar os sistemas para utilização de dispositivos específicos. Deve ser mantido um inventário de tais dispositivos.	**2**
13.8	Proteger	Gerenciar Mídia Externa	Configurar os sistemas para não gravar dados em mídia externa removível, caso não haja requisito de negócio que exija tais dispositivos.	**3**
13.9	Proteger	Criptografar Dados em Dispositivos USB	Caso seja necessária a utilização de dispositivos de armazenamento USB, todos os dados devem ser armazenados de forma criptografada.	**3**

CIS Controle 14: Acesso Controlado com base na Necessidade de Saber

Utilize processos e ferramentas para rastrear / controlar / prevenir / corrigir o acesso seguro a ativos críticos (por exemplo, informações, recursos, sistemas) de acordo com a determinação formal de quais pessoas, computadores e aplicativos têm necessidade e direito de acessar esses ativos críticos com base em uma classificação aprovada.

CIS Controle 14: Acesso Controlado com base na Necessidade de Saber

Subcontrole ID	NIST CSF	Linha de Base	Detalhamento do Controle de Segurança Crítico	Grupo de Implementação
14.1	Proteger	Segmentar a Rede Baseada na Classificação	Segmentar a rede com base na identificação ou nível de classificação das informações armazenadas nos servidores, posicionando todas as informações sensíveis (incluindo os dados pessoais) em *Virtual Local Area Networks* (VLANs) distintas.	**1**
14.2	Proteger	Habilitar Filtragem por Firewall entre VLANs	Habilitar a filtragem por firewall entre VLANs para garantir que apenas sistemas autorizados sejam capazes de se comunicar com outros sistemas necessários para cumprir suas responsabilidades específicas.	**1**
14.3	Proteger	Desativar Comunicação entre Estações de Trabalho	Desativar todas as comunicações entre estações de trabalho para limitar a capacidade de um invasor de se mover lateralmente e comprometer os sistemas vizinhos, por meio de tecnologias como VLANs privadas ou microssegmentação.	**3**

14.4	Proteger	Criptografar Dados Sensíveis em Trânsito	Criptografar todas as informações sensíveis (incluindo dados pessoais) em trânsito.	**2**
14.5	Detectar	Utilizar Ferramenta de Descoberta Ativa para Identificar Dados Sensíveis	Utilizar uma ferramenta de descoberta ativa para identificar todas as informações sensíveis (incluindo dados pessoais) armazenadas, processadas ou transmitidas pelos sistemas de tecnologia da instituição, incluindo aquelas localizadas internamente ou em um provedor de serviços remoto, e atualizar o inventário de informações sensíveis da instituição.	**3**
14.6	Proteger	Proteger a Informação através de Listas de Controle de Acesso	Proteger todas as informações armazenadas por meio de listas de controle de acesso específicas, para servidores de arquivo, compartilhamentos de rede ou bases de dados. Esses controles devem impor o princípio de que apenas indivíduos autorizados devem ter acesso às informações com base em sua necessidade de acesso como parte de suas responsabilidades.	**1**
14.7	Proteger	Impor Controle de Acesso por Ferramenta Automatizada	Utilizar uma ferramenta automatizada, como o *Data Loss Prevention* (DLP) com base em host, para impor controles de acesso aos dados, mesmo quando os dados são copiados para fora do sistema.	**2**
14.8	Proteger	Criptografar Informações Sensíveis	Criptografar todas as informações sensíveis (incluindo dados pessoais) armazenadas usando de uma ferramenta que exija um mecanismo de autenticação secundário não integrado ao sistema operacional, de forma a permitir o acesso às informações.	**3**
14.9	Detectar	Registrar Logs de Acesso ou Mudanças em Dados Sensíveis	Impor registro de log de auditoria detalhado para acesso ou alteração de dados sensíveis ou pessoais (utilizando ferramentas como *File Integrity Monitoring* (FIM) ou *Security Information and Event Monitoring* (SIEM)).	**3**

CIS Controle 15: Controle e Acesso à Rede sem Fio

Utilize processos e ferramentas para rastrear / controlar / prevenir / corrigir a utilização segura de redes locais sem fio (WLANs), pontos de acesso e sistemas clientes sem fio.

CIS Controle 15: Controle e Acesso à Rede sem Fio

Subcontrole ID	NIST CSF	Linha de Base	Detalhamento do Controle de Segurança Crítico	Grupo de Implementação
15.1	Identificar	Manter um Inventário dos Pontos de Acesso Sem Fio Autorizados	Manter um inventário dos pontos de acesso sem fio com conexão autorizada à rede cabeada.	**2**
15.2	Identificar	Detectar Pontos de Acesso Sem Fio Não Autorizados na Rede Cabeada	Configurar ferramentas de varredura de vulnerabilidade de rede para detectar e alertar sobre pontos de acesso sem fio não autorizados conectados à rede cabeada.	**2**
15.3	Detectar	Utilizar WIDS	Utilizar um Sistema de Detecção de Intrusão em Redes sem Fio (*Wireless Intrusion Detection System*, WIDS) para detectar e alertar sobre pontos de acesso sem fio não autorizados conectados à rede cabeada.	**2**
15.4	Proteger	Desabilitar Acesso Sem Fio Não Necessário	Desabilitar o acesso à rede sem fio em dispositivos que não têm uma necessidade de negócio que justifique tal acesso.	**3**

15.5	Proteger	Limitar Acesso Sem Fio em Máquinas Clientes	Configurar o acesso a redes sem fio em máquinas clientes que efetivamente tenham necessidade deste tipo de acesso com base em requisitos de negócio, de forma a permitir o acesso somente a redes sem fio autorizadas e restringir o acesso a quaisquer outras redes sem fio.	**3**
15.6	Proteger	Desabilitar Acesso *Peer-to-Peer*	Desabilitar a capacidade de acesso a redes sem fio *peer-to-peer* (adhoc) em equipamentos clientes.	**2**
15.7	Proteger	Criptografar Dados em Trânsito sobre Redes Sem Fio	Utilizar o padrão *Advanced Encryption Standard* (AES) para criptografar dados em trânsito sobre redes sem fio.	**1**
15.8	Proteger	Utilizar Protocolos de Autenticação para Autenticação Mútua	Garantir que as redes sem fio usem protocolos de autenticação, como o *Extensible Authentication Protocol-Transport Layer Security* (EAP/TLS), que requer autenticação mútua.	**3**
15.9	Proteger	Desabilitar Acesso Periférico Sem Fio (NFC, Bluetooth etc.)	Desabilitar o acesso periférico sem fio de dispositivos (como Bluetooth e *Near Field Communication* (NFC)), a menos que tal acesso seja necessário para fins de negócio.	**2**
15.10	Proteger	Criar Rede Sem Fio Separada	Criar uma rede sem fio separada para dispositivos pessoais ou não confiáveis. O acesso corporativo a partir desta rede deve ser tratado como não confiável e filtrado e auditado apropriadamente.	**1**

CIS Controle 16: Monitoramento e Controle de Credenciais de Acesso

Gerencie ativamente o ciclo de vida das contas do sistema e do aplicativo - sua criação, utilização, inatividade, exclusão - a fim de minimizar as oportunidades de aproveitamento pelos invasores.

CIS Controle 16: Monitoramento e Controle de Credenciais de Acesso

Subcontrole ID	NIST CSF	Linha de Base	Detalhamento do Controle de Segurança Crítico	Grupo de Implementação
16.1	Identificar	Manter um Inventário dos Sistemas de Autenticação	Manter um inventário de cada um dos sistemas de autenticação da instituição, incluindo aqueles localizados internamente ou em um provedor de serviços remoto.	**2**
16.2	Proteger	Configurar Ponto de Autenticação Centralizado	Configurar o acesso para todas as contas por meio do menor número possível de pontos centralizados de autenticação, incluindo sistemas de rede, segurança e sistemas em nuvem.	**2**
16.3	Proteger	Exigir Autenticação Multifator	Exigir autenticação multifator para todas as contas de usuário, em todos os sistemas, quer gerenciados internamente ou por terceiros.	**2**
16.4	Proteger	Criptografar ou Aplicar Hash em Todas as Credenciais	Aplicar criptografia ou *hash* com um *salt* em todas as credenciais de autenticação quando armazenadas.	**2**

16.5	Proteger	Criptografar Transmissão de Credenciais e Nomes de Usuários	Garantir que todos os nomes de conta de usuário e credenciais de autenticação sejam transmitidos pela rede utilizando canais criptografados.	**2**
16.6	Identificar	Manter Inventário de Contas	Manter um inventário de todas as contas organizadas por sistema de autenticação.	**2**
16.7	Proteger	Estabelecer Processo de Revogação de Contas	Definir e utilizar um processo automatizado para a revogação de direitos de acesso a sistemas desabilitando imediatamente as contas no momento do término do vínculo e trabalho ou da alteração das responsabilidades de um funcionário ou prestador de serviços contratado. Desabilitar tais contas, ao invés de excluí-las, permite a preservação de trilhas de auditoria.	**2**
16.8	Proteger	Desabilitar Contas Sem Uso	Desabilitar qualquer conta que não possa ser associada a um processo de negócios ou usuário.	**1**
16.9	Proteger	Desabilitar Contas Sem Uso por Tempo	Desabilitar automaticamente contas inativas após um determinado período de inatividade.	**1**
16.10	Proteger	Configurar Período de Expiração	Garantir que todas as contas tenham uma data de expiração que seja configurada e monitorada.	**2**
16.11	Proteger	Bloquear Estações de Trabalho por Inatividade	Bloquear automaticamente a estação de trabalho após um período pré-definido de inatividade.	**1**
16.12	Detectar	Monitorar Tentativas de Acessar Conta Desativada	Monitorar as tentativas de acessar contas desativadas por meio do registro de auditoria.	**2**
16.13	Detectar	Alertar Desvio de Comportamento	Alertar quando os usuários se desviam do comportamento normal de login, como hora do dia, localização da estação de trabalho e duração.	**3**

CIS Controle 17: Implementar Programa de Conscientização e Treinamento em Segurança

Para toda força de trabalho na instituição (priorizando aquelas pessoas que lidem com missão crítica para o negócio e sua segurança), identifique os conhecimentos, habilidades e capacidades específicas necessárias para apoiar a defesa da empresa; desenvolver e executar um plano integrado para avaliar, identificar lacunas e remediá-las por meio de políticas, planejamento institucional, treinamento e programas de conscientização.

CIS Controle 17: Implementar Programa de Conscientização e Treinamento em Segurança

Subcontrole ID	NIST CSF	Linha de Base	Detalhamento do Controle de Segurança Crítico	Grupo de Implementação
17.1	Identificar	Identificar Lacunas de Conhecimento	Realizar uma análise de lacunas de conhecimento de forma a compreender que conhecimentos e comportamentos não estão sendo alcançados pela equipe, utilizando esta informação para elaborar uma trilha de educação.	**2**
17.2	Proteger	Realizar Treinamento para Suprir Lacunas de Conhecimento	Realizar treinamentos para suprir as lacunas de conhecimento identificadas, de forma a impactar positivamente o comportamento da equipe com relação à segurança.	**2**
17.3	Proteger	Criar Programa de Conscientização de Segurança	Criar programa de conscientização de segurança para que todos os membros da força de trabalho concluam regularmente para 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.	**1**
17.4	Proteger	Atualizar Programa de Conscientização	Garantir que o programa de conscientização de segurança da instituição seja atualizado com frequência (pelo menos anualmente) para lidar com novas tecnologias, ameaças, padrões e requisitos de negócios.	**2**
17.5	Proteger	Treinar Força de Trabalho em Autenticação Segura	Treinar os membros da força de trabalho sobre a importância de habilitar e utilizar a autenticação segura.	**1**
17.6	Proteger	Treinar Força de Trabalho em Identificar Ataque de Engenharia Social	Treinar a força de trabalho sobre como identificar diferentes formas de ataques de engenharia social, como phishing, golpes de telefone e chamadas realizadas por impostores.	**1**
17.7	Proteger	Treinar Força de Trabalho em Manipular Dados Sensíveis	Treinar os membros da força de trabalho sobre como identificar e armazenar, transferir, arquivar e destruir informações sensíveis (incluindo dados pessoais) adequadamente.	**1**
17.8	Proteger	Treinar Força de Trabalho em Exposição de Dados Não Intencional	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**
17.9	Proteger	Treinar Força de Trabalho em Identificar e Relatar um Incidente	Treinar os membros da força de trabalho para serem capazes de identificar os indicadores mais comuns de um incidente e serem capazes de relatar tal incidente.	**1**

CIS Controle 18: 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.

CIS Controle 18: Segurança de Aplicações

Subcontrole ID	NIST CSF	Linha de Base	Detalhamento do Controle de Segurança Crítico	Grupo de Implementação
18.1	Proteger	Definir Práticas Seguras de Codificação	Definir práticas seguras de codificação apropriadas para a linguagem de programação e o ambiente de desenvolvimento que está sendo utilizado na instituição.	**2**
18.2	Proteger	Garantir Verificação Explícita de Erros	Para software desenvolvido internamente, garantir que a verificação explícita de erros seja realizada e documentada para todas as entradas, incluindo tamanho, tipo e intervalos de dados, formatos aceitáveis, entre outros.	**2**
18.3	Proteger	Verificar Suporte de Softwares Adquiridos	Verificar se a versão de todo o software adquirido de fora da instituição ainda é compatível com o desenvolvedor ou adequadamente reforçada com base nas recomendações de segurança do desenvolvedor.	**2**
18.4	Proteger	Utilizar apenas Componentes Atualizados e Aprovados	Utilizar apenas componentes de terceiros aprovados e atualizados para os desenvolvimentos realizados pela instituição.	**2**
18.5	Proteger	Utilizar Algoritmos de Criptografia Amplamente Aceitos no Mercado	Utilizar apenas algoritmos de criptografia padronizados, atualmente aceitos e amplamente revisados.	**2**
18.6	Proteger	Treinar Equipe de Desenvolvimento em Código Seguro	Garantir que todos os responsáveis pelo desenvolvimento de software recebam treinamento para escrever código seguro para seu ambiente de desenvolvimento e responsabilidades específicas.	**2**
18.7	Detectar	Aplicar Ferramentas de Análise Estática e Dinâmica de Código	Aplicar ferramentas de análise estática e dinâmica para verificar se as práticas de codificação seguras estão sendo seguidas para os softwares desenvolvidos internamente.	**2**
18.8	Proteger	Estabelecer Processo de Aceite e Endereçamento de Relatos de Vulnerabilidade em Software	Estabelecer 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.	**2**
18.9	Proteger	Separar Ambientes de Produção e Não Produção	Manter ambientes separados para sistemas de produção e não produção. Os desenvolvedores não devem ter acesso não monitorado aos ambientes de produção.	**2**
18.10	Proteger	Implantar Firewall de Aplicação Web	Proteger as aplicações web implantando firewalls de aplicação web (*Web Application Firewalls* - WAFs) que inspecionam todo o tráfego que flui para a aplicação web em busca de ataques a aplicações comuns. Para aplicações que não são baseadas no acesso web, firewalls de aplicação específicos devem ser implantados se essas ferramentas estiverem disponíveis para o tipo de aplicação fornecida. Se o tráfego for criptografado, o dispositivo deve ficar atrás da criptografia ou ser capaz de descriptografar o tráfego antes da análise. Se nenhuma das opções for apropriada, um firewall de aplicação web baseado em host deve ser implantado.	**2**
18.11	Proteger	Utilizar Configurações Modelos de Segurança para	Para aplicações que dependem de um banco de dados, utilizar modelos de configuração de proteção padronizado. Todos os sistemas que fazem parte de processos críticos de negócios também devem ser testados.	**2**

		Banco de Dados		

CIS Controle 19: Gerenciamento e Resposta a Incidentes

Proteja as informações da instituição, bem como sua reputação, desenvolvendo e implementando uma infraestrutura de resposta a incidentes (por exemplo, planos, papéis definidos, treinamento, comunicações, supervisão de gerenciamento) para descobrir rapidamente um ataque e, em seguida, conter efetivamente o dano, erradicando a presença do invasor, e restaurando a integridade da rede e dos sistemas.

CIS Controle 19: Gerenciamento e Resposta a Incidentes

Subcontrole ID	NIST CSF	Linha de Base	Detalhamento do Controle de Segurança Crítico	Grupo de Implementação
19.1	Proteger	Documentar Procedimentos de Resposta a Incidente	Garantir que existem planos de resposta a incidentes por escrito que definem as responsabilidades dos envolvidos, bem como as fases de tratamento / gerenciamento de incidentes.	1
19.2	Proteger	Atribuir Deveres no Tratamento de Incidentes	Definir cargos e responsabilidades para o tratamento de incidentes em computadores e redes para indivíduos específicos e garantir o acompanhamento e documentação ao longo da resolução do incidente.	2
19.3	Proteger	Designar Responsável de Nível Gerencial	Designar responsáveis de nível gerencial, bem como substitutos, que apoiarão o processo de tratamento de incidentes, atuando em papéis de tomada de decisão.	1
19.4	Proteger	Elaborar Processo de Comunicação	Elaborar processos de comunicação com tempo necessário para que os administradores do sistema e outros membros da força de trabalho relatem eventos anômalos à equipe de tratamento de incidentes, os mecanismos para tais relatórios e o tipo de informação que deve ser incluída na notificação de incidente.	2
19.5	Proteger	Manter Contato de Terceiros para Relatar Incidente de Segurança	Reunir e manter informações sobre contato de terceiros a serem utilizadas para relatar um incidente de segurança, como autoridades policiais, departamentos governamentais relevantes, fornecedores e parceiros.	1
19.6	Proteger	Publicar Incidentes de Segurança para Conscientizar Força de Trabalho	Publicar informações para todos os membros da força de trabalho, a respeito de relatórios de anomalias e incidentes em computadores resolvidos pela equipe de tratamento de incidentes. Essas informações devem ser incluídas nas atividades rotineiras de conscientização dos colaboradores.	1
19.7	Proteger	Treinar Equipe de Resposta a Incidentes em Cenários de Ameaças	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.	2
19.8	Proteger	Criar Pontuação e Modelo de Priorização para Incidentes	Criar um processo com pontuação para a priorização de incidentes com base no impacto conhecido ou potencial sobre a instituição. Utilizar a pontuação para definir a frequência das atualizações de status e procedimentos de escalonamento.	3

CIS Controle 20: Testes de Invasão e Exercícios de "Red Team"

Teste a força da defesa da instituição (a tecnologia, os processos e as pessoas) simulando os objetivos e ações de um invasor.

CIS Controle 20: Testes de Invasão e Exercícios de "Red Team"

Subcontrole ID	NIST CSF	Linha de Base	Detalhamento do Controle de Segurança Crítico	Grupo de Implementação
20.1	Proteger	Estabelecer um Programa de Teste de Invasão	Estabelecer um programa para testes de invasão que inclua um escopo completo de ataques combinados, como ataques sem fio, baseados em cliente e aplicações web.	**2**
20.2	Detectar	Conduzir Testes Internos e Externo Regularmente	Conduzir testes de invasão internos e externos regularmente para identificar vulnerabilidades e vetores de ataque que podem ser utilizados para explorar sistemas corporativos com sucesso.	**2**
20.3	Detectar	Realizar Exercícios Periódicos com o "Red Team"	Realizar exercícios periódicos com o "Red Team" (equipes dedicadas a realizar testes de invasão) para testar a prontidão institucional para identificar e interromper ataques ou para responder com rapidez e eficácia.	**3**
20.4	Detectar	Incluir Testes para Detectar Informações Sensíveis	Incluir testes para detectar a presença de sistemas de informação desprotegidos e artefatos que possam ser úteis para eventuais atacantes, incluindo diagramas de rede, arquivos de configuração, relatórios de testes de invasão antigos, e-mails ou documentos que contenham senhas ou outras informações críticas para a operação dos sistemas.	**2**
20.5	Detectar	Simular o Ambiente Real e Aplicar Testes de Invasão	Criar um ambiente de testes que simule um ambiente de produção para testes de invasão e ataques do "Red Team" contra elementos que não são normalmente testados em produção, como ataques contra supervisão de controles e aquisição de dados, e outros sistemas de controle.	**2**
20.6	Detectar	Utilizar Ferramentas de Varreduras e Testes de Invasão em Conjunto	Utilizar ferramentas de verificação de vulnerabilidade e teste de invasão em conjunto. Os resultados das avaliações de varredura de vulnerabilidade devem ser usados como um ponto de partida para orientar e focar os esforços de teste de invasão.	**2**
20.7	Detectar	Documentar os Resultados do "Red Team" em Padrões Abertos	Sempre que possível, garantir que os resultados do "Red Team" sejam documentados utilizando padrões abertos e legíveis por máquina (por exemplo, SCAP). Elaborar um método de pontuação para determinar os resultados dos exercícios do "Red Team" para que os resultados possam ser comparados ao longo do tempo.	**3**
20.8	Detectar	Controlar e Monitorar Contas Associadas em Testes de Invasão	Quaisquer contas de usuário ou sistema utilizadas para realizar testes de invasão devem ser controladas e monitoradas para garantir que estejam sendo utilizadas apenas para fins legítimos e sejam removidas ou restauradas à função normal após o término do teste.	**2**

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, mas os cálculos e a organização da planilha 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 quatro tipos de planilhas:

Planilha	Função	
LeiaME	Apresenta informações gerais sobre a planilha, organização e definição dos campos.	
Dashboard	Apresenta um painel gerencial com resumos gráficos das principais informações preenchidas nos 20 controles, como: porcentagem de implementação dos controles, porcentagem por grupo do NIST CSF, por grupo de implementação, entre outros.	
CSC #1 a CSC #20	Cada uma das planilhas apresenta os subcontroles de um determinado controle, conforme distribuição do CIS.	
Value	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.	

Abaixo são descritos os campos que são encontrados nas planilhas:

Campos	Função
ID	Este é o número de identificação (ID) do subcontrole e o vincula a cada um dos 20 Controles de Segurança Crítico, adaptado da documentação CIS-Controls-Version-7-1. .
Detalhamento do Controle de Segurança Crítico	Este campo detalha cada subcontrole específico, adaptado da documentação CIS-Controls-Version-7-1. .
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 do subcontrole para basilar a implementação.
Política Aprovada	Indica se a instituição tem uma política definida que aponta que eles devem implementar o subcontrole definido.
Controle Implementado	Determina se a instituição atualmente implementou ou não o subcontrole e em que grau o controle foi implementado.
Controle Automatizado	Determina se a instituição atualmente automatizou ou não a implementação deste subcontrole, e em que grau o controle foi automatizado.
Controle Reportado à Direção	Determina se os responsáveis pela implementação estão reportando este subcontrole aos representantes da alta direção, e em que grau o controle foi reportado.
Subcontroles Adequados	Concentra informações sobre a adequação de um controle em um índice, em que, quanto mais próximo de 0%, menos adequado os subcontroles estão e, quanto mais próximo de 100%, mais adequados estão. As informações concentradas retratam o status dos subcontroles presentes em uma política definida, seu status de implementação, seu status de automatização ou imposição técnica e o reporte à alta direção.
Subcontroles Não Adequados	Concentra informações sobre a não adequação de um controle em um índice, em que quanto mais próximo de 0%, mais adequados os subcontroles estão e, quanto mais próximo de 100%, menos adequados estão. As informações concentradas retratam o status dos subcontroles 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, mas compõe ao fim um índice de maturidade, em que todas as pontuações de nível de maturidade são somadas. As tabelas abaixo 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 20.
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. Índice de Maturidade = Pontuação Nível 1 + Pontuação Nível 2 + Pontuação Nível 3 + Pontuação Nível 4 + Pontuação Nível 5. Quanto mais próxima a pontuação é de um, maior é a maturidade da instituição no tema segurança da informação em relação aos 20 controles do CIS.

A maioria dos subcontroles 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 um dos subcontroles				
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 subcontroles daquele nível avaliado. A tabela abaixo simula, apenas como exemplo prático, essa representação para o Controle de Segurança Crítico 5 do CIS (CSC 5):

ID	Política Aprovada	Controle Implementado	Controle Automatizado	Controle Reportado à Direção
5.1	Política Informal (0,25)	Não Implementado (0)	Não Aplicável (Não Contabilizado)	Não Aplicável (Não Contabilizado)
5.2	Política Escrita (0,75)	Implementada em Alguns Sistemas (0,5)	Não Aplicável (Não Contabilizado)	Não Aplicável (Não Contabilizado)
5.3	Política Aprovada (1)	Implementada em Muitos Sistemas (0,75)	Automatizada em Alguns Sistemas (0,5)	Reportada em Muitos Sistemas (0,75)
5.4	Política Parcialmente Escrita (0,5)	Partes da Política Implementadas (0,25)	Automatizada em Alguns Sistemas (0,5)	Não Reportada (0)
5.5	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 20 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 um dos subcontroles 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	%
Subcontroles Adequados	(Política Aprovada + Controle Implementado + Controle Automatizado + Reportado à Direção)/4	(0,5+0,4+0,33+0,25)/4 = 0,37	37%
Subcontroles Não Adequados	1 – Subcontroles Adequados	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 os subcontroles analisados.
2	Controles 1 a 5 Implementados	Média dos pesos de todos os subcontroles implementados dos controles de 1 a 5.
3	Todos os Controles Implementados	Média dos pesos de todos os subcontroles implementados dos controles de 6 a 20.
4	Todos os Controles Automatizados	Média dos pesos de todos os subcontroles automatizados dos controles de 1 a 20.
5	Todos os Controles Reportados	Média dos pesos de todos os subcontroles reportados à direção dos controles de 1 a 20.

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

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.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **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.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27005:2019**: Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação. Rio de Janeiro, 2019.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **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.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **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.

AUDITSCRITPS. 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.

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

INTERNATIONAL STANDARD. **ISO/IEC 29134:2017**: Information technology – Security techniques – Guidelines for privacy impact assessment. Genebra, 2017.

INTERNATIONAL STANDARD. **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_web.pdf >. Acesso em: 28 fev. 2021.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **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.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **NIST Special Publication 800-53 revisão 5**: Security and Privacy Controls for Information Systems and Organizations. Gaithersburg, 2020.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. NIST - 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.