Modelo de Política de Gerenciamento de Vulnerabilidades

PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO (PPSI)

Versão 2.0

Brasília, março de 2023

MODELO DE POLÍTICA DE GERENCIAMENTO DE VULNERABILIDADES

MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS

Esther Dweck
Ministra

SECRETARIA DE GOVERNO DIGITAL

Rogério Souza Mascarenhas
Secretário de Governo Digital

DIRETORIA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

Leonardo Rodrigo Ferreira
Diretor de Privacidade e Segurança da Informação

COORDENAÇÃO-GERAL DE PROTEÇÃO DE DADOS

Loriza Andrade Vaz de Melo
Coordenadora-Geral de Proteção de Dados

Equipe Técnica de Elaboração

Francisco Magno Felix Nobre
Ivaldo Jeferson de Santana Castro
Raphael César Estevão

Equipe Revisora

Luiz Henrique do Espírito Santo Andrade
Rogério Vinicius Matos Rocha
Romário César de Almeida

Equipe Técnica de Revisão – Versão 2.0

Francisco Magno Felix Nobre
Julierme Rodrigues da Silva
Rogério Vinicius Matos Rocha

Histórico de Versões

Data	Versão	Descrição	Autor
22/07/2022	1.0	Política de Gerenciamento de Vulnerabilidades	Equipe Técnica de Elaboração
31/03/2022	2.0	Atualização para alinhamento com o Guia do Framework de Privacidade e Segurança da Informação, conforme destacado no Anexo I.	Equipe Técnica de Atualização

Sumário

Aviso Preliminar e Agradecimentos

O presente Modelo, especialmente recomendado e dirigido aos órgãos e às entidades da Administração Pública Federal - APF, visa a auxiliar na Elaboração de uma Política de Gerenciamento de Vulnerabilidades, em atendimento ao previsto no art. 46 da Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), que determina que a Administração Pública, ao prestar diversos serviços que tratam dados pessoais à sociedade, deve adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito dos dados que estão sob sua custódia. Adicionalmente, a Elaboração de uma Política de Gerenciamento de Vulnerabilidades visa a atender, além da LGPD, a outros normativos vigentes sobre o tema de privacidade e segurança da informação.

Este documento é de autoria exclusiva da Secretaria de Governo Digital (SGD) do Ministério da Gestão e da Inovação em Serviços Públicos e tem como referência fundamental o Guia do Framework de Privacidade e Segurança da Informação baseado em diversas publicações e documentos técnicos já existentes que são utilizados amplamente por profissionais da área de privacidade e segurança da informação. Destacam-se as publicações do Center for Internet Security (CIS), da International Organization for Standardization (ISO) e do National Institute of Standards and Technology (NIST). Com o objetivo de facilitar a difusão de conhecimentos sobre privacidade e segurança da informação, tais referências, quando escritas em línguas estrangeiras, foram traduzidas para o português pela equipe técnica da Diretoria de Privacidade e Segurança da Informação da Secretaria de Governo Digital.

Nesse cenário, a Secretaria de Governo Digital enfatiza que:

a) não representa, tampouco se manifesta em nome do CIS, da ISO e do NIST e vice-versa;
b) não se manifesta em nome de autoridades de privacidade e segurança da informação;
c) não é coautora das publicações internacionais abordadas;
d) não assume nenhuma responsabilidade administrativa, técnica ou jurídica por usos ou interpretações inadequadas, fragmentados ou parciais do presente modelo; e
e) caso o leitor deseje se certificar de que atende integralmente os requisitos das publicações das instituições mencionadas, deverá consultar diretamente as fontes oficiais de informação ofertadas por elas, que foram listadas na seção “Referência Legal e de Boas Práticas” deste documento.

Finalmente, um agradecimento especial deve ser registrado ao CIS, à ISO, ao NIST e aos profissionais de privacidade e segurança da informação consultados, por suas valiosas contribuições para a comunidade e para elaboração deste documento.

Este Modelo será atualizado frequentemente, de acordo com as novas diretrizes determinadas pelas autoridades em privacidade e segurança da informação ou segundo eventuais alterações que ocorram nos normativos vigentes relacionados a privacidade e segurança da informação e outras referências utilizadas neste documento.

Introdução

Este Modelo tem por finalidade apresentar orientações com o intuito de auxiliar os órgãos e entidades da Administração Pública Federal, direta, autárquica e fundacional a elaborar sua Política de Gerenciamento de Vulnerabilidades no âmbito institucional.

O Controle 7 do Guia do Framework de Privacidade e Segurança da Informação (p. 45) estabelece que:

__Controle 7: Gestão Contínua de Vulnerabilidades__ – Desenvolver um plano para avaliar e rastrear vulnerabilidades continuamente em todos os ativos dentro da infraestrutura da organização, a fim de remediar e minimizar a janela de oportunidade para atacantes. Monitorar as fontes públicas e privadas para novas informações sobre ameaças e vulnerabilidades.

O presente documento serve como um modelo prático a ser utilizado para auxiliar na adoção do Controle 7 do Guia do Framework de Privacidade e Segurança da Informação[1] v1 e respectivas evoluções desta versão (1.1, 1.2 etc.) elaborado e publicado pela SGD. As medidas do Controle 7 que estão contempladas por este modelo são: 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7.

Hoje, mais do que em qualquer outro momento da história, o Governo utiliza a tecnologia para melhorar e expandir a oferta de serviços públicos para o cidadão apoiado em sistemas informatizados.

Nesse contexto, os órgãos federais brasileiros, com infraestrutura própria ou contratada de terceiros, coletam, recebem, acessam, processam, modificam, produzem, extraem, validam, armazenam, distribuem e transmitem informações confidenciais e públicas para apoiar a entrega de produtos e serviços essenciais. Exemplos disso são: fornecimento de serviços financeiros; fornecimento de serviços de emissões guias, certificados e carteiras; processamento de autorizações de segurança ou dados de saúde; fornecimento de serviços em nuvem; desenvolvendo comunicações via cabo, wireless e/ou satélites; e sistemas militares de defesa. As informações federais são frequentemente fornecidas ou compartilhadas, obedecidos os requisitos legais, com entidades como governos estaduais e municipais, empresas públicas e privadas, faculdades e universidades, organizações de pesquisa independentes ou públicas e organizações do terceiro setor.

A proteção dessas informações pelo Governo enquanto agente de tratamento está designada no **art. 46 da Lei Geral de Proteção de Dados**, sancionada em 14 de agosto de 2018:

> *"Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito."*

Importante ressaltar que adoção deste modelo não dispensa o órgão de considerar as diretrizes gerais estabelecidas para implementação da Política de Segurança da Informação, conforme prevê o art.12, Inciso IV

[1] < https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_framework_psi.pdf >. Acesso em 03/02/2023.

da Instrução Normativa Nº 01/GSI/PR, bem como os Capítulos III e IV da Instrução Normativa Nº 03/GSI/PR, de 28 de maio de 2021, a qual dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal.

O gerenciamento de vulnerabilidades é o processo de busca, priorização e correção de vulnerabilidades em sistemas e software institucionais. A Política de Gerenciamento de Vulnerabilidade fornece os processos e procedimentos para governar o ciclo de vida do gerenciamento de vulnerabilidades e assim garantir que os ativos da instituição não contenham vulnerabilidades. Esta política se aplica a todos os departamentos e todos os ativos conectados à rede institucional.

Política de Gerenciamento de Vulnerabilidades

IMPORTANTE: Este modelo de Política de Gerenciamento de Vulnerabilidades deve ser utilizado exclusivamente como referência, devendo o órgão ou a entidade interessada considerar as particularidades técnicas específicas do seu ambiente, bem como observar a boa aderência aos processos internos, a fim de construir uma política que seja adequada à sua realidade.

Este modelo tem por enfoque prover diretrizes para Política de Gerenciamento de Vulnerabilidades, com o propósito de atender a necessidade de implementar os controles emergenciais previstos no Anexo 5 do Programa de Privacidade e Segurança da Informação (PPSI). Não obstante, recomenda-se que o órgão ou a entidade considere, no mínimo, as diretrizes gerais estabelecidas para implementação da Política de Segurança da Informação, conforme prevê o art. 12, inciso IV da Instrução Normativa Nº 01/GSI/PR, bem como os Capítulos III e IV da Instrução Normativa Nº 03/GSI/PR, de 28 de maio de 2021, a qual dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal.

Para usar este modelo, basta substituir o texto em cinza itálico por informações personalizadas de seu órgão ou entidade. Quando a escrita for finalizada, recomenda-se igualmente a exclusão de todos os textos introdutórios em cinza não itálico (ou de exemplo) e a conversão de todo o texto restante em preto antes do processo de aprovação.

Responsável	*Nome da pessoa ou área responsável pela gestão desta política.*
Aprovado por:	*Nome da pessoa ou área responsável pela aprovação e autorização da implementação desta política.*
Políticas relacionadas	*Relacione outras políticas corporativas relacionadas dentro do modelo ou a ele externas. Exemplos: Política de Gestão de Riscos / Política de Backup e Restauração de Dados Digitais / Política de Segurança da Informação (POSIN).*
Localização de armazenamento	*Descreva a localização física ou digital das cópias desta política.*
Data da aprovação	*Liste a data em que a política entrou em vigor.*
Data de revisão	*Liste a data em que a política deve passar por revisão e atualização. Recomenda-se que seja definido um período de revisão da política, pelo menos um ano, ou quando houver alterações de normativos legais significativos sobre o tema.*
Versão	*Indique a versão atual desta política*

Propósito [Objetivo da Política] conforme IN01 GSI/PR art.11

Levando em consideração a natureza e a finalidade do órgão ou da entidade, descreve os fatores ou circunstâncias que determinam a existência da política de gerenciamento de vulnerabilidades. Além disso, informe os objetivos básicos da política e o que ela pretende alcançar. Exemplo:

O objetivo da Política de Gerenciamento de Vulnerabilidades é estabelecer as regras relacionadas às atividades de identificação, avaliação, documentação, gestão, comunicação e remediação de vulnerabilidades. Além disso, contempla ações e boas práticas que devem ser observadas para se evitar que vulnerabilidades estejam presentes nos ativos da organização.

A revisão, a avaliação, a aplicação e a verificação das atualizações de ativos de informação auxiliam a mitigar as vulnerabilidades no ambiente de Tecnologia da Informação e Telecomunicações, bem como os riscos associados a tais vulnerabilidades.

Escopo [Amplitude, alcance da Política] conforme IN01 GSI/PR art.12 item I

Defina a quem e a quais sistemas esta política se aplica. Liste os agentes públicos e colaboradores necessários para cumprir ou simplesmente indique "todos" se todos devem cumprir. Também indique quaisquer exclusões

ou exceções que estejam fora de escopo, ou seja, essas pessoas, elementos ou situações que não estejam cobertas por esta política ou onde uma consideração especial possa ser feita.

Esta política de gerenciamento de vulnerabilidades se aplica aos sistemas e ativos informacionais *[do órgão ou entidade]*, incluindo funcionários, gestores, prestadores de serviços e contratados que tenham acesso e/ou utilizem ativos informacionais.

Os serviços de TI críticos *[do órgão ou entidade]* devem ser formalmente elencados pelo *[citar o responsável pela definição, ex.: Comitê de Gestão de Tecnologia da Informação do órgão ou entidade]*.

Já ficam previamente estabelecidos os *[citar tipo ou nome dos processos ou sistemas críticos],* como serviços críticos da *[organização]*.

O *[departamento/coordenação de TI do órgão ou entidade]* é responsável por elaborar, manter e fazer cumprir a Política de Gerenciamento de Vulnerabilidades *[no órgão ou entidade]*.

Exceções

Pode ocorrer que alguns ativos de informação da *[informar o nome do órgão ou entidade]* não serem contemplados por possíveis dificuldades técnicas ou obrigações contratuais e normativas. Quaisquer exceções a esta política deverão ser documentadas e aprovadas por meio de um processo de gerenciamento de exceções da *[informar o nome do órgão ou entidade]*.

É importante salientar que tais exceções precisam ser tratadas no mapeamento de riscos de segurança da informação que o órgão ou a entidade deve efetuar em cumprimento ao Capítulo III da Instrução Normativa GSI/PR Nº 3, de 28 de maio de 2021.

Público

Esta Política de Gerenciamento de Vulnerabilidades (PGV) *[do órgão ou entidade]* se aplica a indivíduos responsáveis pela gestão e a indivíduos que utilizam qualquer Ativo de Informação da Rede Computadores em nome *[do órgão ou entidade]*. Além disso, a presente política se aplica a quaisquer provedores e entidades terceirizadas com acesso a informações, redes e aplicativos *[do órgão ou entidade]*.

Termos e Definições [Glossário] conforme PORTARIA GSI/PR Nº 93

Defina quaisquer termos-chave, siglas ou conceitos que serão utilizados na política. [Sugere-se utilizar como referência as definições apresentadas na Portaria GSI/PR Nº 93, de 18 de outubro 2021 – Glossário de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República]. Exemplo:

AMEAÇA – Conjunto de fatores externos com o potencial de causarem dano para um sistema ou organização.

ANÁLISE DE VULNERABILIDADES – Verificação e exame técnico de vulnerabilidades, para determinar onde estão localizadas e como foram exploradas.

ATIVOS DE INFORMAÇÃO – Meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, recursos humanos que a eles têm acesso e conhecimento ou dado que tem valor para um indivíduo ou organização.

BANCO DE DADOS – Coleção de dados inter-relacionados, representando informações sobre um domínio específico. São coleções organizadas de dados que se relacionam, a fim de criar algum sentido (informação) e de dar mais eficiência durante uma consulta ou a geração de informações ou conhecimento.

CTIR GOV – Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, subordinado ao Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República.

CVE (*Common Vulnerabilities and Exposures*) – Vulnerabilidades e Exposições Comuns.

CVSS (*Common Vulnerability Scoring System*) – Sistema comum de pontuação de vulnerabilidade.

HOST – Um computador ou dispositivo de TI (por exemplo, roteador, switch, gateway, firewall).

ID CVE – Identificação para um CVE específico.

GERENCIAMENTO DE VULNERABILIDADE – Processo cíclico e contínuo de identificação, avaliação, documentação, gestão, comunicação e remediação de vulnerabilidades.

GESTÃO DE MUDANÇAS NOS ASPECTOS RELATIVOS À SEGURANÇA DA INFORMAÇÃO – Processo estruturado que visa aumentar a probabilidade de sucesso em mudanças, com mínimos impactos, e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação.

GESTOR DE SEGURANÇA DA INFORMAÇÃO – Responsável pelas ações de segurança da informação no âmbito do órgão ou entidade da administração pública federal.

LOG (REGISTRO DE AUDITORIA) – Registro de eventos relevantes em um dispositivo ou sistema computacional.

NTP (*Network Time Protocol*) – Protocolo de Tempo para Redes.

PATCH – Uma parte de código adicional desenvolvido para resolver um problema ou falha em um software existente.

PENTEST – Acrônimo de teste de penetração (*penetration test*).

REMEDIAÇÃO – O ato de corrigir uma vulnerabilidade ou eliminar uma ameaça.

RISCO – No sentido amplo, trata-se da possibilidade de ocorrência de um evento que pode impactar o cumprimento dos objetivos. Pode ser mensurado em termos de impacto e de probabilidade.

RISCO DE SEGURANÇA DA INFORMAÇÃO – Risco potencial associado à exploração de uma ou mais vulnerabilidades de um ou mais ativos de informação, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização.

TESTE DE INVASÃO – Metodologia para testar a eficácia e a resiliência de ativos através da identificação e exploração de fraquezas nos controles de segurança e da simulação das ações e objetivos de um atacante.

TESTE DE PENETRAÇÃO (PENTEST) – Também chamado de teste de intrusão, é fundamental para a análise de vulnerabilidades e consiste em testar todos os sistemas em busca de, além das já verificadas na fase anterior, vulnerabilidades conhecidas e disponibilizadas por especialistas ou pelas instituições detentoras dos softwares que estão sendo utilizados pelo órgão ou entidade.

VULNERABILIDADE – Condição que, quando explorada por um criminoso cibernético, pode resultar em uma violação de segurança cibernética dos sistemas computacionais ou redes de computadores, e consiste na interseção de três fatores: suscetibilidade ou falha do sistema, acesso possível à falha e capacidade de explorar essa falha.

Referência legal e de boas práticas [Documentos norteadores]

Se for aplicável, liste quaisquer leis, regulamentos ou guias de boas práticas que regem a política ou com as quais a política deve estar em conformidade ou ser cumprida. Confirme com a respectiva consultoria jurídica do órgão ou da entidade se a lista é completa e precisa.

Orientação	Seção
Decreto 10.332/2020 - Estratégia de Governo Digital 2020-2022	Em sua íntegra
Decreto Nº 10.046/2019 - Governança no Compartilhamento de Dados (GCD)	Art. 2º, inciso XXIII
Decreto Nº 10.222/2020 - Estratégia Nacional de Segurança Cibernética (E-CIBER)	Anexo, Item 2.3.4 e 2.3.5
Decreto Nº 9.573/2018 - Política Nacional de Segurança de Infraestruturas Críticas (PNSIC)	Anexo, art. 3º, Inciso I, II e V

Decreto Nº 9.637/2018 - Política Nacional de Segurança da Informação (PNSI)	CAPÍTULO I - Art. 2º, Incisos III e IV CAPÍTULO II - Art. 3º, Inciso III, IV, VIII XI CAPÍTULO VI - Seção IV – Art. 15
Framework Control Objectives for Information and Related Technology – Cobit, conjunto de boas práticas a serem aplicadas à governança da TI	v4.1: DS11: Gerenciar Dados v5: DSS01.01, DSS04.08; DSS06.04, DSS04.08, DSS05.06; DSS06.05-06, DSS04.08, DSS001.01; DSS05.02-05; DSS06.03; DSS06.06
Framework de segurança cibernética do CIS 8	Salvaguardas do controle 7 (*Continuous Vulnerability Management*), controle 11 (*Data Recovery Capabilities*), e controle 18 (*Penetration Testing*)
Framework Information Technology Infrastructure Library – ITIL, v. 4, conjunto de boas práticas a serem aplicadas na infraestrutura, operação e gerenciamento de serviços de TI	Gestão da Segurança da Informação
Guia de Framework de Privacidade e Segurança da Informação (PPSI)	Controle 7 em sua íntegra
Instrução Normativa 01/GSI/PR	Art. 12, Inciso IV, alíneas g, h
Instrução Normativa Nº 03/GSI/PR, de 28 de maio de 2021	Capítulo IV
Lei Nº 13.709/2018 – Lei Geral de Proteção de Dados	CAPÍTULO VII - Seção I – art. 46, Seção II - art. 50
Lei Nº 12.527/2011 – Lei de Acesso à Informação (LAI)	Em sua íntegra
Norma ABNT NBR ISO/IEC 27001:2013 Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos	A.12.3 Cópias de segurança
Norma ABNT NBR ISO/IEC 27002:2013 Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação	12.3 Cópias de segurança 18 Conformidade
National Institute of Standards and Technology (NIST)	CSF: SP 800-40 Rev.2, *Creating a Patch and Vulnerability Management Program* CSF: SP 800-40 Rev 4, *Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology*
Portaria GSI/PR nº 93, de 18 de outubro de 2021	Em sua íntegra
Guia de Gerenciamento de Vulnerabilidades SGD	Em sua íntegra
NGINX.org	Correções de bugs
Office of the Chief Technology Officer – OCTO	Política de gerenciamento de vulnerabilidades
Vulnerability Management Policy Template for CIS Control 7	Em sua íntegra

Declarações da política [Regras aplicáveis ao caso específico]

Descreva as regras que compõem a política. Isso normalmente toma a forma de uma série de breves declarações prescritivas e proscritivas. A subdivisão desta seção em subseções pode ser necessária, dependendo do comprimento ou complexidade da política. Exemplo:

Os sistemas e os dispositivos conectados à rede [do órgão ou entidade], sejam eles próprios ou aqueles em processo de desenvolvimento e suporte por terceiros, devem passar periodicamente por varreduras em busca de vulnerabilidades que possam representar um risco para a infraestrutura e os dados sensíveis [do órgão ou entidade].

Novos aplicativos/sistemas construídos pela equipe de desenvolvimento [do órgão ou entidade] ou de terceiros devem ser verificados no que concerne a vulnerabilidades antes de serem implantados no ambiente de produção.

Processo de gerenciamento de vulnerabilidades (PGV)

1. Um processo de Gerenciamento de Vulnerabilidades (PGV) deve ser criado, implementado, mantido e aplicado [no órgão ou entidade].
2. O processo deve conter a implementação de mecanismos para obter informações oportunas sobre vulnerabilidades técnicas dos sistemas e ativos de informação, a avaliação da exposição da organização a tais vulnerabilidades e a implementação de salvaguardas apropriadas para lidar com o risco associado.
3. O processo deve contemplar o gerenciamento de vulnerabilidades dos diversos ativos que sustentam os serviços da organização, como a ativos que compõe a rede da organização, aplicações web, aplicativos móveis, sistemas operacionais, dentre outros.
4. O processo deve incluir atividades de suporte, incluindo, mas não se limitando a métricas de relatório e treinamento para implementação eficaz do PGV.
5. O processo deve incluir funções e responsabilidades das equipes/funções para realizar todas as atividades de maneira oportuna e eficaz para [o órgão ou entidade].
6. O processo deve estabelecer mecanismos para obter atualizações de software quando emitidas pelo fabricante ou fornecedor oficial regularmente utilizando recursos autorizados, tais como sites de fornecedores de sistemas, fóruns e grupos de notícias, bancos de dados de gerenciamento de vulnerabilidades e diferentes ferramentas para rastrear as vulnerabilidades mais recentes.
7. A consistência e a eficácia do processo devem ser medidas por meio de métricas de gerenciamento de vulnerabilidades.
8. As métricas de gerenciamento de vulnerabilidades devem ser definidas pelo [Comitê de Segurança da Informação ou estrutura equivalente] e suas medições devem ser apresentadas a cada [período].

Em síntese, as métricas são medidas baseadas em uma ou mais referências que servem para mensurar o grau de vulnerabilidade/ameaça em um determinado ativo de informação ou infraestrutura de TI.

Algumas das métricas fundamentais (e não exaustivas) cujo acompanhamento é recomendado em uma estratégia de gerenciamento de vulnerabilidades abrangem: cobertura, tempo de detecção, tempo de permanência, tempo para contenção ou atenuação, número médio de vulnerabilidades ao longo do tempo, eficiência no gerenciamento de patches e resultados de correção em relação aos SLAs da tabela de priorização de vulnerabilidades.

Mapeamento de ativos de informação

9. Um mapeamento de ativos de informação deve constar no escopo do processo de gerenciamento de vulnerabilidades e patches para determinar qual marca, modelo e versão de equipamento de hardware, sistemas operacionais, banco de dados, sistema, servidor web e aplicativos de software são usados [no órgão ou entidade].

10. O mapeamento de ativos de informação deve ser atualizado [periodicamente] ou sempre que ocorrerem alterações significativas para garantir que os recursos informacionais estejam cobertos pelo processo de gerenciamento de vulnerabilidades [do órgão ou entidade].

Detecção de vulnerabilidades

As principais ações relacionadas à detecção de vulnerabilidades têm como enfoque definir e refinar o escopo que será avaliado; preparar as ferramentas necessárias e verificar sua integridade; e realizar testes e verificar resultados.

Tenha em mente que uma detecção eficaz de vulnerabilidades deve ser capaz de encontrar vulnerabilidades e reportá-las em tempo hábil para sua correção, de forma a impedir que sejam exploradas.

Recomenda-se que as verificações de vulnerabilidade cubram os ativos internos e externos à rede de produção.

11. As funções e as responsabilidades das equipes/funções para realizar atividades de detecção de vulnerabilidades devem ser estabelecidas.
12. As ferramentas devem ser configuradas e ajustadas adequadamente de acordo com o escopo avaliado.
13. Os tipos de varreduras e os tipos de teste devem ser avaliados e ajustados para que sejam congruentes com o escopo avaliado.
14. A frequência de testes de segurança deve levar em consideração os requisitos legais, regulamentares e contratuais que *[o órgão ou entidade]* deve cumprir e os riscos associados aos ativos avaliados.
15. As varreduras de vulnerabilidades na rede corporativa devem ser realizadas por períodos determinados ou após alteração significativa na rede, por equipe interna ou por terceiro ou uma combinação de ambos.
16. Os testes de segurança devem utilizar o feed de vulnerabilidade mais recente, de forma a evitar que determinadas vulnerabilidades não sejam detectadas.
17. Para cada teste, é necessário verificar a integridade da ferramenta utilizada e se ela varreu corretamente os ativos analisados e se existem exceções de vulnerabilidades.
18. As ferramentas utilizadas devem ser ajustadas continuamente, de forma a evitar que varreduras feitas por ferramentas distintas gerarem resultados distintos.
19. O teste de invasão ou o teste de penetração (Pentest) deve ser realizado conforme critério de necessidade *[do órgão ou entidade]* ou pelo menos *[período]*, utilizando especialistas qualificados externos como parte de um exercício planejado, que inclui o escopo da avaliação, os métodos de uso e os requisitos operacionais, a fim de fornecer as informações mais precisas e relevantes sobre as vulnerabilidades atuais, sem afetar o funcionamento normal *[do órgão ou entidade]*.
20. A integridade do resultado de detecção de vulnerabilidades deve ser avaliada antes de sua comunicação, de forma a evitar inconsistências, contradições ou resultados incompletos.
21. A detecção manual de vulnerabilidades deve ser considerada como complemento à detecção automática de vulnerabilidades.

Para informações mais detalhadas sobre Testes de Invasão, recomendamos a leitura do **Guia do Framework de Segurança, CIS Controle 18 (Testes de Invasão)**[2].

Elaboração e manutenção dos relatórios

22. A *[equipe de gerenciamento de vulnerabilidades]* deve elaborar relatórios após cada ciclo de detecção para auxiliar *[o órgão ou entidade]* a entender e mensurar as vulnerabilidades existentes.

[2] https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias-operacionais-para-adequacao-a-lei-geral-de-protecao-de-dados-pessoais-lgpd

23. Os resultados da varredura devem passar por análise da *[equipe de gerenciamento de vulnerabilidades]* com o dispositivo ou gerenciador de rede para que possíveis falsos positivos possam ser identificados e eliminados.
24. Grupos de ativos de informação devem ser determinados por tipo de ambiente, por tipo de sistema, por ID CVE ou por tipo de vulnerabilidade.
25. A *[equipe de gerenciamento de vulnerabilidades]* deve adotar métricas para os relatórios de vulnerabilidade e determinar o valor percentual dos ativos de informação vulneráveis por gravidade e CVSS.
26. A quantidade e a porcentagem de novas vulnerabilidades devem ser monitoradas por: severidade; grupos funcionais; tipo de ambiente; tipo de sistema; autoridade de numeração CVE; e tipo de vulnerabilidade.
27. O relatório deve ser classificado, durante e após a sua elaboração, de acordo com a sensibilidade das informações presentes nele.
28. Todas as versões do relatório devem ser remetidas ao *[Comitê de Segurança da Informação]* gestor(a) de segurança de informação.

Banco de dados de vulnerabilidades

É importante saber que o gerenciamento de vulnerabilidades deve ser capaz de produzir e manter um banco de dados de vulnerabilidades coletadas de todas as suas fontes. Este banco de dados de vulnerabilidades poderá ser utilizado durante a priorização e a correção de vulnerabilidades.

29. Deve ser mantido um banco de dados de vulnerabilidades coletadas de várias fontes, como sites de segurança da informação, boletins de segurança ou publicações de fornecedores de software, que precisam ser aplicadas aos sistemas e ativos informacionais *[do órgão ou entidade]*.
30. O banco de dados poderá incluir informações de vulnerabilidade, análise de vulnerabilidade para priorização e plano de correção de vulnerabilidade.
31. O banco de dados deve ser atualizado regularmente com as informações mais recentes. As novas vulnerabilidades devem ser adicionadas ao banco de dados tão logo forem descobertas.
32. É recomendável que o banco de dados de vulnerabilidades seja integrado com outras ferramentas de segurança, como scanners de vulnerabilidades e sistemas de gerenciamento de patches. Isso ajuda a identificar e corrigir vulnerabilidades de forma mais rápida e eficiente.
33. As informações coletadas no banco de dados de vulnerabilidades devem ser analisadas regularmente para identificar tendências e padrões visando a tomada de medidas proativas para evitar futuras vulnerabilidades.

Priorização e correção de vulnerabilidades

O monitoramento proativo de vulnerabilidades e ameaças em dispositivos, se remediadas, reduzirá ou eliminará o potencial de exploração e economizará os recursos necessários para responder a incidentes após a exploração.

34. O tratamento de vulnerabilidades deve ser priorizado com base em sua classificação de risco e criticidade, tempo esperado para correção, grau de risco, impacto em caso de exploração e no valor que o ativo ou host impactado tem para o negócio *[do órgão ou entidade]*.

35. As vulnerabilidades devem ser tratadas de acordo com o seu nível de severidade e nos prazos estipulados abaixo. Exemplo de classificação:

Nível de severidade	Prazo de correção	Descrição do risco
Muito Crítico (6)	*Até [2 dias]*	*Condição totalmente inaceitável quando medidas imediatas devem ser tomadas para eliminar a materialização do risco e mitigar perigos e impactos.*
Crítico (5)	*Até [30 dias]*	*Pessoas mal-intencionadas podem facilmente obter o controle do host, o que pode comprometer toda a sua rede. As vulnerabilidades incluem acesso de leitura e gravação a arquivos, execução remota de comandos e backdoors.*
Alto (4)	*Até [45 dias]*	*Pessoas mal-intencionadas podem obter o controle do host ou coletar informações altamente confidenciais, incluindo acesso de "leitura" ao arquivo, backdoors em potencial ou uma lista de todas as contas de usuário no host.*
Médio (3)	*Até [90 dias]*	*Pessoas mal-intencionadas podem obter acesso às configurações de segurança no host, o que pode levar ao acesso a arquivos e à divulgação de conteúdo de arquivos, navegação em diretórios, ataques de negação de serviço e uso não autorizado de serviços.*
Baixo (2)	*Até [120 dias]*	*Pessoas mal-intencionadas podem coletar informações confidenciais do host, como versões de software instaladas, que podem revelar vulnerabilidades conhecidas.*
Muito baixo (1)	*Até 180 dias*	*Pessoas mal-intencionadas podem coletar informações sobre o host por meio de portas ou serviços abertos, o que pode levar à divulgação de outras vulnerabilidades.*

É fundamental que o órgão ou a entidade seja capaz de estabelecer essa classificação de risco de acordo com suas demandas e necessidades internas.

36. Os testes que forem concluídos com falha devem ser examinados novamente até que sua execução seja concluída com êxito. Caso não seja possível, deve-se avaliar se a vulnerabilidade será incluída na lista de exceções por pessoal autorizado, com base no processo de aceitação de risco.

37. Devem-se estabelecer mecanismos para obter atualizações de software quando emitidas pelo fabricante ou fornecedor oficial regularmente, utilizando recursos autorizados, tais como sites de fornecedores de sistemas, fóruns e grupos de notícias, bancos de dados de gerenciamento de vulnerabilidades e diferentes ferramentas para rastrear as vulnerabilidades mais recentes.

38. Quando as vulnerabilidades não puderem ser corrigidas dentro do prazo estabelecido no item 35, *[a equipe de gerenciamento de vulnerabilidades]* deve enviar uma “solicitação de renúncia” ao *[departamento/coordenação de segurança da informação do órgão ou entidade]*. A solicitação deve conter as seguintes informações:

    - Detalhes do sistema ou ativo.
    - Descrição detalhada da vulnerabilidade
    - Avaliação de risco que justifique a não correção imediata
    - A justificativa clara pela qual a correção não pode ser realizada no prazo estabelecido.
    - Detalhes dos controles existentes (se houver).
    - Novo prazo de correção.
    - Plano de ação da remediação (obedecendo o novo prazo de correção).

A decisão de aceitar ou rejeitar a solicitação de renúncia deve ser tomada pelo(a) *[departamento/coordenação de segurança da informação do órgão ou entidade]*, com base na avaliação de risco apresentada. Se a solicitação de renúncia for aceita, a vulnerabilidade deve ser monitorada continuamente, pautado pelo plano de ação apresentado devendo ser corrigida assim que possível.

39. Os alertas de vulnerabilidades, as correções de patches e as ameaças emergentes que correspondam aos recursos informacionais relacionados no inventário de sistema e ativos de informação devem ser monitorados.

Das exceções

Importante ressalvar que estas exceções precisam ser tratadas no mapeamento de riscos de segurança da informação que o órgão ou entidade deve efetuar em cumprimento ao Capítulo III da Instrução Normativa GSI/PR Nº 3, de 28 de maio de 2021.

O objetivo é garantir que as exceções à política de gerenciamento de vulnerabilidades sejam tratadas de forma transparente e consistente, minimizando os riscos potenciais e protegendo adequadamente os ativos de informação da organização.

40. Para os ativos de informação *[do órgão ou entidade]* não contemplados por esta política em função de dificuldades técnicas ou obrigações contratuais e normativas ou outras razões legítimas, as exceções deverão ser documentadas e aprovadas por meio de um processo de gerenciamento de exceções *[do órgão ou entidade].*
41. A lista de exceções de ativos de informação deve ter validade de *[período]*, devendo ser revisada após esse período.

Dos registros de logs

42. Identificar quais eventos dos ativos de informação devem ser registrados, com base nos requisitos regulatórios, nas melhores práticas e nos objetivos da *[do órgão ou entidade]*.
43. Ativos, físicos ou virtuais, como servidores e recursos de rede, devem recuperar informações baseadas em tempo de uma única fonte de tempo de referência (servidor NTP) regularmente para que os relógios de registro sejam consistentes.
44. As configurações referentes a ativos de informação devem incluir configurações de log para registrar ações que possam afetar ou que sejam relevantes para a segurança da informação.
45. Definir procedimento para análise de logs, como ferramentas de análise e correlação, para identificar possíveis ameaças e vulnerabilidades.
46. Uma revisão dos arquivos de registro (logs) deve ser conduzida pelo menos *[período].*
47. Os arquivos de registro (logs) devem ser protegidos contra adulteração e acesso não autorizado ou exfiltração.
48. Registros de logs dos sistemas e ativos informacionais classificados como críticos devem ser mantidos por pelo menos *[período]*, tempo suficiente para cumprir os requisitos regulatórios e permitir a detecção de ameaças passadas.
49. Monitorar regularmente os registros de logs para identificar quaisquer tentativas de exploração de vulnerabilidades.
50. Registros de log devem ser excluídos de forma segura, garantindo que os registros sejam completamente apagados sem deixar vestígios ou dados remanescentes.

Comunicação da ocorrência de vulnerabilidades e correções

51. As vulnerabilidades e respectivas informações de correção devem ser informadas aos usuários afetados, incluindo, mas não se limitando a: administradores de sistema, proprietários de sistema e usuários finais.
52. As correções bem-sucedidas de vulnerabilidades poderão ser testadas por meio de verificação de vulnerabilidades de rede e host, verificação de logs de patches, testes de invasão/penetração (Pentest) e verificação das definições de configuração.

Implementação e verificação das correções de vulnerabilidades

A implementação e verificação das correções de vulnerabilidades envolvem um processo contínuo e iterativo de identificação, correção e monitoramento das vulnerabilidades para garantir a proteção contra ameaças de segurança da informação.

53. As correções de vulnerabilidades devem ser verificadas a saber se não há novas vulnerabilidades introduzidas. Isso pode ser feito por meio de testes de penetração, testes de vulnerabilidade e análise de logs.
54. Somente correções de vulnerabilidades que foram efetivamente testadas e aprovadas devem ser implantadas em produção. Atividades de correção de vulnerabilidades geralmente incluem, mas não se limitam à instalação de patches de segurança, bem como a ajustes de configuração e/ou remoção de software.
55. Quando instalações de patches de segurança e ajustes de configuração são recomendadas para mitigar as vulnerabilidades, elas devem ser enviadas por meio do *[processo de gestão de mudanças]* para que os controles apropriados sejam implementados para teste, avaliação de riscos e reparação.

Dos serviços em nuvem ou de terceiros

56. Para serviços em nuvem, as responsabilidades do provedor de serviços em nuvem pública com o cliente do serviço em nuvem devem ser definidas e acordadas.
57. Terceiros devem cumprir os requisitos desta Política de Gerenciamento de Vulnerabilidades (PGV). Sempre que possível, essa obrigação e outras responsabilidades que envolvam o gerenciamento de vulnerabilidades devem ser incluídas em contratos com terceiros.

Procedimentos Relevantes

Considere criar documentos de procedimento formal que reforcem e apoiem as declarações políticas acima. Note que é uma prática recomendada abrigar políticas e procedimentos em documentos separados para manter o conteúdo focado e reduzir o número de vezes que a política deve ser renovada pela alta administração.

Um exemplo de documento que possui procedimentos relevantes e que pode ser consultado é o **Guia de Gerenciamento de Vulnerabilidades**[3] presente na página de guias e modelos da SGD.

[3] https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_gerenciamento_vulnerabilidades.pdf

ANEXO I

Mudanças da versão 2.0

Este anexo tem a finalidade de fornecer os destaques das mudanças inseridas nesta versão do Modelo de Política de Gerenciamento de Vulnerabilidades.

Primeiramente, ressalta-se que as mudanças inseridas nesta versão em comparação com a anterior visam a adequação do mesmo com o Guia do Framework de Privacidade e Segurança da Informação v1 elaborado e publicado pela SGD em novembro de 2022.

Foram realizadas inclusões de: seção sobre aviso preliminar e agradecimentos; e referência de que controle e medidas do Framework de Privacidade e Segurança da Informação são atendidos pelo Modelo de Política de Gerenciamento de Vulnerabilidades.

Além disso, foram realizadas as seguintes inclusões para alinhamento com as medidas do Guia do Framework de Privacidade e Segurança da informação citadas a seguir:

- Foram removidas e incluídas novas referências na seção “Referência legal e de boas práticas”;
- Foram feitos ajustes e novas inclusões de itens nas seções “Priorização e correção de vulnerabilidades”, “Banco de dados de vulnerabilidades”, “Das exceções”, “dos Registros de Log” e “Implementação e verificação das correções de vulnerabilidades”.