Modelo de Política de Defesas contra Malware

PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO (PPSI)

Versão 1.1

Brasília, junho de 2024

MODELO DE POLÍTICA DEFESAS CONTRA MALWARE

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 PRIVACIDADE

Julierme Rodrigues da Silva

Coordenadora-Geral de Privacidade

COORDENAÇÃO-GERAL DE SEGURANÇA DA INFORMAÇÃO

Loriza Andrade Vaz de Melo

Coordenadora-Geral de Segurança da Informação

Equipe Técnica de Elaboração

Bruno Pierre Rodrigues de Sousa

Francisco Magno Felix Nobre

Leonard Keyzo Yamaoka Batista

Ivaldo Jeferson de Santana Castro

Rafael da Silva Ribeiro

Raphael César Estevão

Equipe Revisora

Adriano de Andrade Moura

Rodrigo Duran Lima

Rogério Vinicius Matos Rocha

Equipe de Revisão - Versão 1.1

Adriano de Andrade Moura

Anderson Souza de Araújo

Rogério Vinicius Matos Rocha

Histórico de Versões

Data	Versão	Descrição	Autor
14/05/2024	1.0	Modelo de Política de Defesas Conta Malware	Equipe Técnica de Elaboração
18/06/2024	1.1	Atualização para melhor atender as medidas 12.3 e 12.4 do Guia do Framework de Privacidade e Segurança da Informação, conforme destacado no Anexo I.	Equipe Técnica de Revisão

Sumário

Aviso Preliminar e Agradecimentos 6
Introdução 7
Política de Defesas Contra Malware 10
Propósito [Objetivo da Política] conforme IN01 GSI/PR Art.11 10
Escopo [Amplitude, alcance da Política] conforme IN01 GSI/PR Art.12 item I 11
Termos e Definições [Glossário] conforme IN01 GSI/PR Art.12 item II 11
Referência legal e de boas práticas [Documentos norteadores] 11
Declarações da política [Regras aplicáveis ao caso específico] 12
Não conformidade 23
Concordância 23
ANEXO I 24

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 Defesas contra Malware, 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 Defesas contra Malware 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 Defesas contra Malware no âmbito institucional.

O Controle 10 do Guia do Framework de Privacidade e Segurança da Informação (p. 47, 50) estabelece que:

> ***Controle 10: Defesas contra Malware -*** *Impedir ou controlar a instalação, disseminação e execução de aplicações, códigos ou scripts maliciosos em ativos da organização.*
>
> ***Controle 12: Gestão da Infraestrutura de Redes*** *- Estabeleça, implemente e gerencie ativamente (rastreie, reporte, corrija) os dispositivos de rede, a fim de evitar que atacantes explorem serviços de rede e pontos de acesso vulneráveis.*

O presente documento serve como um modelo prático a ser utilizado para auxiliar na adoção dos Controles 10 e 12 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 dos Controles 10 e 12 que estão contempladas por este Modelo são: 10.1, 10.2, 10.3, 10.4, 10.5, 10.6, 10.7, 12.3 e 12.4.

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, 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 (por exemplo, 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; 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 da Instrução Normativa Nº 01/GSI/PR, bem como os Capítulos III e IV da Instrução Normativa Nº 03/GSI/PR, de 28

1 < https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_framework_psi.pdf >. Acesso em 15/04/2024.

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 malware é uma das ameaças mais comuns que uma organização pode enfrentar. Esta ameaça pode ser usada para capturar credenciais, roubar dados, identificar outros alvos na rede e criptografar ou destruir dados. O malware entra em uma organização por meio de vulnerabilidades internas em dispositivos de usuários finais, anexos de e-mail, páginas da Web, serviços em nuvem, dispositivos móveis, mídias removíveis e muito mais. Frequentemente, o malware depende do comportamento inseguro do usuário final, como clicar em links, abrir anexos, instalar software ou perfis ou, ainda, inserir unidades flash USB (Universal Serial Bus) nos sistemas. O malware moderno é projetado para evitar, enganar e desativar as defesas. Portanto, as defesas contra malware devem ser capazes de operar em um ambiente dinâmico por meio de automação, atualização oportuna e rápida e integração com outros processos, como gerenciamento de vulnerabilidades e resposta a incidentes. As defesas devem ser implantadas em todos os pontos de entrada e ativos institucionais possíveis para detectar, prevenir a propagação ou controlar a execução de software ou código malicioso.

Existem muitos tipos de malware, incluindo:

- **Vírus**: Uma seção oculta e autorreplicante de software de computador, geralmente lógica maliciosa, que se propaga infectando (ou seja, inserindo uma cópia de si mesmo e tornando-se parte dele) outro programa. Um vírus não pode funcionar sozinho; requer que seu programa host seja executado para tornar o vírus ativo.
- **Trojan**: Um programa útil ou aparentemente útil que contém código oculto de natureza maliciosa que é executado quando o programa é invocado.
- **Ransomware**: software malicioso usado para criptografar os dados de uma empresa e exigir pagamento para restaurar o acesso.
- **Spyware**: Software que é instalado secreta ou sub-repticiamente num sistema de informação para recolher informações sobre indivíduos ou empresas sem o seu conhecimento; um tipo de código malicioso.

A defesa contra malware é o processo de adotar medidas preventivas de segurança para se proteger e assim evitar que ataques de malwares sejam bem-sucedidos, isto inclui a configuração, manutenção, detecção, geração de relatórios e correção de software antimalware e do malware que ele identifica.

Existem muitos tipos de defesas contra malware, incluindo:

- **Detecção baseada em assinatura**: software antimalware projetado para baixar rotineiramente uma lista de malwares conhecidos como nocivos e colocar em quarentena ou remover instâncias desse malware quando eles são identificados em um ativo corporativo.
- **Detecção baseada em heurística**: um conjunto de regras ou algoritmos desenvolvidos especificamente para detectar malware. Às vezes, essas regras podem ser usadas para identificar comportamentos maliciosos em malware nunca vistos.
- **Software de detecção de intrusão baseado em host (HIDS)**: software antimalware que monitora o comportamento dinâmico e o estado do sistema para identificar se há malware presente no sistema. Isto inclui monitorar as comunicações que entram e saem do sistema.
- **Sistema de detecção de intrusões (IDS) baseado em rede**: software antimalware ou um dispositivo de rede dedicado que monitora e analisa o tráfego de rede.
- **Sistemas de prevenção de intrusões (IPS) baseados em rede**: software antimalware ou um dispositivo de rede dedicado que monitora e analisa o tráfego de rede e, em seguida, dá um passo extra para realmente bloquear o tráfego suspeito e malicioso.
- **Lista de permissões ou lista de bloqueio de aplicativos**: software ou recursos antimalware integrados ao sistema operacional que permitem ou negam explicitamente a execução de software, bibliotecas ou scripts.

- **Detecção e resposta de endpoint (EDR)**: uma coleção de ferramentas que analisa, detecta e responde a eventos em um sistema para identificar malware, utilizando vários recursos antimalware no mesmo sistema. Este aplicativo monitora continuamente eventos no sistema em busca de sinais de infecção. Eventos normais no sistema são registrados e analisados para estabelecer uma linha de base para que hábitos comuns possam ser identificados e eventos anormais possam ser relatados.

Observe que qualquer pacote ou suíte antimalware provavelmente aproveitará várias tecnologias desta lista.

A política de defesas contra malware fornece diretrizes e boas-práticas para realizar essas tarefas, objetivando orientar o órgão da melhor maneira possível contra estes ataques, de acordo com sua realidade.

Política de Defesas Contra Malware

IMPORTANTE: Este modelo de Política de Defesas Contra Malware deve ser utilizado exclusivamente como referência, devendo o órgão considerar as particularidades técnicas especificas do seu ambiente, bem como observar a boa aderência aos processos internos, a fim de construir uma política que seja adequada a sua realidade.

Este modelo tem por foco prover diretrizes para a Defesa contra Malware, a fim de atender a necessidade de implementar os controles e medidas destacados pelas orientações constantes da seção de introdução deste documento. Contudo, recomenda-se que o órgão considere, no mínimo, as diretrizes gerais estabelecidas para implementação, conforme prevê o Art.12, Inciso IV, alínea d da Instrução Normativa Nº 01/GSI/PR, bem como o Capítulo II 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 por informações personalizadas do seu órgão ou entidade. Quando estiver concluído, exclua todos os textos introdutórios ou de exemplos e converta 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 ou externas a este modelo, por exemplo: POSIN
Localização de armazenamento	Descreva a localização física ou digital das cópias desta política.
Data da Aprovação	Liste a data em que essa política entrou em vigor.
Data de revisão	Liste a data em que esta política deve passar por revisão e atualização.
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 entidade, descreva os fatores ou circunstâncias que determinam a existência da política de defesas contra malware. Além disso, afirme os objetivos básicos da política e o que a política pretende alcançar.

Exemplo: O objetivo desta política é garantir a proteção adequada contra malware em todos os ativos de informação e que os controles de proteção recomendados para estes ativos de informação estejam em vigor.

Em sua missão, o(a) [Órgão ou Entidade] deve assegurar a segurança e a continuidade do negócio por meio da adoção de defesas antimalware atualizadas e aplicadas em todos os pontos de entrada e ativos da instituição. Isso é essencial para identificar e impedir a disseminação ou gerenciar a execução de softwares ou códigos mal-intencionados.

Os ativos de informação do(a) [Órgão ou Entidade] devem ser classificados a fim de permitir a definição de níveis de segurança para eles. Cada ativo de informação deverá ter um “proprietário”, o qual realizará a classificação do ativo de informação, registrando-o em uma base de dados gerenciada de forma centralizada.

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.

Exemplo:

Esta Política de Defesas Contra Malware se aplica a todos os processos de negócios e dados, sistemas de informação e componentes, pessoal e áreas físicas do(a) Órgão ou Entidade.

Esta política se aplica em todos os possíveis pontos de entrada e ativos institucionais para detectar e impedir a propagação ou controlar a execução de software ou código malicioso.

Termos e Definições [Glossário] conforme IN01 GSI/PR Art.12 item II

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 DE 2021 – Glossário de Segurança da Informação do Gabinete de Segurança Institucional da PRESIDÊNCIA DA REPÚBLICA].

Exemplo:

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;

INCIDENTE - interrupção não planejada ou redução da qualidade de um serviço, ou seja, ocorrência, ação ou omissão, que tenha permitido, ou possa vir a permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;

MALWARE - software malicioso, projetado para infiltrar um sistema computacional, com a intenção de roubar dados ou danificar aplicativos ou o sistema operacional. Esse tipo de software costuma entrar em uma rede por meio de diversas atividades aprovadas pela empresa, como e-mail ou sites. Entre os exemplos de malware estão os vírus, worms, trojans (ou cavalos de Troia), spyware, adware e rootkits;

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 o departamento jurídico que a lista é completa e precisa.

Orientação	Seção
Decreto Nº 10.332/2020 - Estratégia de Governo Digital 2020-2022	Em sua íntegra
Decreto Nº 10.046/2019 - Governança no Compartilhamento de Dados (GCD)	Art. 2, 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.3, Inciso I, II e V

Decreto Nº 9.637/2018 - Política Nacional de Segurança da Informação (PNSI)	CAPÍTULO I - Art.2, Incisos III e IV CAPÍTULO II - Art.3, Inciso III, IV, VIII XI CAPÍTULO VI - Seção IV – Art.15
Guia do Framework de Privacidade e Segurança da Informação	Controles 10 e 12
Instrução Normativa Nº 04/GSI/PR, de 26 de março de 2020	Capítulo II
Guias Operacionais SGD	Todos
Instrução Normativa Nº 01/GSI/PR, de 27 de maio de 2020	Art.12, Inciso IV, alínea, e
Instrução Normativa Nº 03/GSI/PR, de 28 de maio de 2021	Capítulo III
Lei Nº 13.709/2018 – Lei Geral de Proteção de Dados	CAPÍTULO VII - Seção I – Art. 46, Seção II Art. 50
NIST SP 800-83 v1	Seções 2, 3 e 4
Norma ABNT NBR ISO/IEC 27002: Segurança da informação, segurança cibernética e proteção à privacidade — Controles de segurança da informação	Seção 8.7
Portaria GSI/PR nº 93, de 18 de outubro de 2021	Em sua íntegra
Malware Defense Policy Template CIS v8 - March 2023	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.

Tenha em mente que as organizações devem garantir que as diretrizes da Política de Defesas Contra Malware abordem a prevenção de incidentes de malware. Essas declarações da política devem ser usadas como base em esforços adicionais de prevenção de malware, como conscientização dos usuários e equipe de TI, mitigação de vulnerabilidades, mitigação de ameaças e arquitetura defensiva.

A Política de Defesas Contra Malware deve ser tão geral quanto possível para proporcionar flexibilidade na sua implementação e reduzir a necessidade de atualizações frequentes, mas também suficientemente específica para tornar claros a intenção e o âmbito da política.

CAPÍTULO I
DOS PRINCÍPIOS GERAIS

Art. 1° A Política de Defesas contra Malware (PDM) deve estar alinhada com à Política de Segurança da Informação do(a) [Órgão ou Entidade].

Art. 2° A PDM deve estar alinhada com uma gestão de continuidade de negócios em nível organizacional.

Art. 3° Esta política apresenta um conjunto de diretrizes para lidar com os incidentes e eventos de malware que porventura possam ocorrer no âmbito institucional. Contudo, isso não anula a necessidade de tratar especificidades de cada tipo. A depender do tipo de malware, pode-se considerar procedimentos diferentes para lidar com incidentes de cada categoria.

Art. 4° O(A) [Órgão ou Entidade] deve implementar políticas que abordam prevenção contra malware.

Art. 5° O(A) [Órgão ou Entidade] deve empenhar-se em detectar e validar ameaças de malware rapidamente para minimizar o número de ativos de informação expostos e a quantidade de danos que possa vir a sofrer.

Art. 6° A PDM deve ser revisada e atualizada regularmente tanto para refletir as mudanças das ameaças e novas tecnologias quanto para garantir que esteja em conformidade com normas e regulamentações vigentes.

Art. 7° A eficácia e efetividade da PDM devem ser avaliadas continuamente por meio de auditorias e análise de eventuais incidentes.

[Acrescentar os princípios que devem ser considerados para a política].

CAPÍTULO II
PAPÉIS E RESPONSABILIDADES

É necessário que o(a) [Órgão ou Entidade] estabeleça de forma clara os papéis e responsabilidades das pessoas envolvidas com a segurança da informação, tais atribuições devem estar de acordo com as políticas de segurança da informação e proteção de dados e as políticas específicas por tema que o(a) [Órgão ou Entidade] venha a elaborar.

Art. 8° Cabe ao [Diretor de TIC] do(a) [Órgão ou Entidade] estabelecer o responsável por garantir que os ativos da informação conectados à rede estejam devidamente instalados, atualizados e protegidos contra malwares.

Art. 9° O [Diretor de TIC]do(a) [Órgão ou Entidade] deve indicar o responsável por realizar a monitoração dos ativos de informação que por algum motivo não estejam de acordo com a esta política de proteção contra malware.

Art. 10 A [Diretoria de TIC] do(a) [Órgão ou Entidade] deve orientar todos os colaboradores e eventuais usuários dos ativos de informação em relação ao cumprimento das diretrizes estabelecidas nesta política.

Art. 11 A [Diretoria de TIC] do(a) [Órgão ou Entidade] deve manter uma relação de todos os aplicativos que podem ser instalados nos ativos de informação.

Art. 12 Os provedores de serviço de TIC do(a) [Órgão ou Entidade] devem garantir que todos os ativos de informação estejam de acordo com as diretrizes estabelecidas nesta política

Art. 13 O(A) [Órgão ou Entidade] deve documentar os procedimentos utilizados na atribuição de responsabilidades para lidar com a proteção nos ativos de informação e recuperação de ataques de malware.

[Acrescentar outras diretrizes que devem ser considerados para a política].

CAPÍTULO III
CONSCIENTIZAÇÃO E TREINAMENTO

É necessário que os colaboradores recebam treinamento em segurança da informação, em consonância com a política de proteção contra malware do(a) [Órgão ou Entidade], a fim de conscientizar-se a respeito da observação das diretrizes e ações a serem tomadas com o objetivo de reduzir os riscos de segurança cibernética decorrentes da exploração das vulnerabilidades por softwares maliciosos.

Art. 14 O Gestor de Segurança da Informação do(a) [Órgão ou Entidade] deve promover ações de conscientização de recursos humanos em temas relacionados à segurança da informação, conforme previsto no art. 19 da Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020.

Art. 15 O(A) [Órgão ou Entidade] deve promover a conscientização ou treinamento a todos os usuários sobre como identificar arquivos e programas infectados por malware e a quem relatar uma possível infecção.

Art. 16 O(A) [Órgão ou Entidade] deve basear-se em relatórios de eventos de malware ocorridos anteriormente para planejar o programa de conscientização e treinamento de seus colaboradores.

Art. 17 Criar e manter um programa de conscientização, educação e treinamento que aborde temas entendidos como importantes, levando em consideração a política de segurança da informação e suas diretrizes.

Art. 18 O programa de conscientização e treinamento sobre malware do(a) [Órgão ou Entidade] deve ser revisado e atualizado de forma periódica.

Art. 19 O(A) [Órgão ou Entidade] deve elaborar treinamentos específicos para os diferentes requisitos de segurança da informação inerentes a cada cargo ou função de seus servidores.

Art. 20 O programa de conscientização e treinamento do(a) [Órgão ou Entidade] deve considerar o treinamento de novos colaboradores.

Art. 21 O(A) [Órgão ou Entidade] deve criar e manter uma forma de avaliação do programa de conscientização e treinamento por meio de feedback dos participantes.

Art. 22 O programa de conscientização e treinamento deve ter como um dos objetivos elucidar os colaboradores sobre as suas responsabilidades no que diz respeito a segurança da informação de ativos de informação do(a) [Órgão ou Entidade].

Art. 23 O programa de conscientização do(a) [Órgão ou Entidade] deve observar a importância de elaborar a conscientização e treinamento dos prestadores de serviço de acordo com novas contratações e encerramento de contrato.

Art. 24 O programa de conscientização do(a) [Órgão ou Entidade] pode utilizar de ferramentas como salas virtuais e físicas de treinamento, folhetos, cartazes, websites, boletins informativos e eventos específicos para manter o público-alvo, informado e atualizado sobre as diretrizes de proteção contra malware do(a) [Órgão ou Entidade].

Art. 25 O(A) [Órgão ou Entidade] deve conscientizar os seus colaboradores quanto a importância de relatar o mais rápido possível uma possível infecção ou evento de segurança da informação.

Art. 26 O(A) [Órgão ou Entidade] deve manter e divulgar de forma ampla o canal de comunicação de possíveis eventos de segurança da informação.

[Acrescentar outras diretrizes que devem ser considerados para a política].

CAPÍTULO IV
PREVENÇÃO DE INCIDENTES DE MALWARE

Esta seção oferece recomendações para prevenir incidentes de malware dentro da instituição. A prevenção de malware estabelece a base para a implementação de controles preventivos, garantindo a proteção dos dados e outros ativos. É fundamental que a defesa contra malware seja respaldada pela conscientização dos usuários

Art. 27 O [Órgão ou Entidade] deve adotar medidas que visam mitigar o impacto da exploração de vulnerabilidades por malwares, tais como a indisponibilidade de recursos (redes, aplicações etc) que venham a afetar negativamente a continuidade dos negócios.

Art. 28 O [Órgão ou Entidade] deve adotar técnicas de segmentação de rede visando mitigar a propagação ou disseminação de ameaças, tais como malwares, dentro da rede da organização.

Art. 29 O [Órgão ou Entidade] deve adotar, quando necessário, infraestrutura como código para a configuração e atualização do ambiente de redes, bem como, implementar protocolos de redes seguros, tais como SSH e HTTPS.

Art. 30 Planos de continuidade de negócios para recuperação de ataques de malware, incluindo backups e softwares necessários, devem ser mantidos pelo(a) [Órgão ou Entidade].

Art. 31 Procedimentos para coletar informações sobre novos malwares, devem ser implementados pelo(a) [Órgão ou Entidade].

Art. 32 Realizar, regularmente e de forma automatizada, backup de todos os dados de sistemas. As cópias de segurança devem ser armazenadas e protegidas em locais adequados, por meio de segurança física ou criptografados. Além disso devem ser executados testes de integridade dos dados e das mídias de armazenamento em período regular.

Art. 33 O(A) [Órgão ou Entidade] deve elaborar e manter uma política de senhas que oriente aos usuários utilizarem senhas fortes e autenticação de múltiplo fator para suas contas e dispositivos. Além disso deve-se utilizar senhas exclusivas para todos os ativos institucionais.

Art. 34 É dever do(a) [Órgão ou Entidade] implementar medidas que detectem o uso de softwares permitidos ou não permitidos.

Art. 35 O(A) [Órgão ou Entidade] deve implementar medidas que detectam acessos a sites maliciosos ou suspeitos.

Art. 36 Logs e alertas do software antimalware devem ser armazenados pelo(a) [Órgão ou Entidade] em um local seguro e o acesso deve ser restrito para evitar roubo ou vazamento de dados pessoais que tenham sido coletados.

Art. 37 O(A) [Órgão ou Entidade] deve especificar tipos de softwares preventivos (antimalware, antivírus, firewall) necessários para cada tipo de host (servidor, laptop, smartphone, pc etc.) e deve listar os requisitos para configuração e atualização deles.

Art. 38 Ameaças para tipos de malware que não exploram vulnerabilidades, como ataques de engenharia social, devem ser mitigados pelo(a) [Órgão ou Entidade].

CAPÍTULO V
CONFIGURAÇÃO E ATUALIZAÇÃO

Art. 39 É dever do(a) [Órgão ou Entidade] manter um processo de configuração seguro para ativos corporativos, dispositivos de usuário final incluindo portáteis e móveis, dispositivos não computacionais/IoT, servidores e softwares como sistemas operacionais e aplicações.

Art. 40 O processo de configuração deve ser revisado e atualizado em períodos predefinidos ou quando ocorrer mudanças significativas no(a) [Órgão ou Entidade] que possam impactar esta medida de segurança.

Art. 41 O(A) [Órgão ou Entidade] deve realizar o gerenciamento de software antimalware, recomendado ser feito de forma centralizada podendo conter agentes do software antimalware em ativos de informação como estação de trabalho e servidores.

Art. 42 É dever do(a) [Órgão ou Entidade] configurar e atualizar o software de detecção antimalware regularmente e realizar varredura nos computadores, servidores e mídias de armazenamento eletrônico incluindo:

I. dados recebidos por meio da rede ou qualquer mídia de armazenamento eletrônico;

II. e-mails, mensagens instantâneas e downloads.

Art. 43 O(A) [Órgão ou Entidade] deve configurar o software antimalware para que ele obtenha as atualizações das bases antimalware de forma automática. Quando isso não puder ser realizado, deve ser devidamente justificado e aprovado pelos responsáveis.

Art. 44 É dever do(a) [Órgão ou Entidade] configurar os dispositivos para a não execução e reprodução automática de mídias removíveis.

Art. 45 O(A) [Órgão ou Entidade] deve configurar os softwares antimalware para realizar a varredura automática de mídias removíveis quando inseridas nos dispositivos.

Art. 46 Devem ser configuradas, pelo(a) [Órgão ou Entidade], as funcionalidades "anti-exploits" que estejam disponíveis nos sistemas operacionais e a implementadas as ferramentas que possam ser configuradas para aplicar proteções sobre um conjunto mais amplo de aplicações e executáveis.

Art. 47 O(A) [Órgão ou Entidade] deve realizar o gerenciamento de controle de acesso em ativos que se conectam remotamente à organização, considerando, mas não se limitando a:

I. Determinar a quantidade de acessos às soluções utilizando recursos de softwares e de rede;

II. Possuir processos de configuração segura de ativos remotos;

III. Certificar-se que os sistemas operacionais, software antimalware e demais aplicações estejam sempre atualizados.

Art. 48 O(A) [Órgão ou Entidade] pode utilizar software antimalware com função holística que tenha a capacidade de monitorar e identificar os comportamentos atípicos de seus ativos de informação.

Art. 49 É dever do(a) [Órgão ou Entidade] realizar a atualização de sistemas operacionais e softwares por meio de gestão automatizada de patches.

Art. 50 O(A) [Órgão ou Entidade] deve configurar o software antimalware no servidor de e-mail para realizar a varredura de anexos e implementar um ambiente virtual controlado para realizar a verificação e abertura de anexos, tais como uma sandbox.

Art. 51 É dever do(a) [Órgão ou Entidade] remover ou alterar contas locais e senhas padrão de sistemas operacionais e softwares para evitar acessos não autorizados.

Art. 52 O(A) [Órgão ou Entidade] deve desativar ou remover serviços desnecessários, principalmente os serviços de rede, pois são vetores adicionais que um malware utiliza para se propagar.

Art. 53 Deve ser configurado, pelo(a) [Órgão ou Entidade], o servidor de e-mail para proibir o envio e recebimento de certos tipos de arquivos (Ex.: .exe.)

CAPÍTULO VI
DETECÇÃO E ANÁLISE DE MALWARE

O malware pode ser distribuído por diferentes meios e adquirir diversas formas, por este motivo o(a) [Órgão ou Entidade] deve ficar atento aos sinais de uma possível ameaça, uma vez que esta pode ocorrer em qualquer local da rede. A detecção de malwares requer atenção, sendo necessárias análises detalhadas que exigem amplo conhecimento técnico e experiência da equipe responsável.

Art. 54 O(A) [Órgão ou Entidade] deve realizar verificação e validação regular de softwares, sistemas críticos e de dados de sistemas em busca de arquivos desconhecidos que não tenham sido aprovados ou alterações não autorizadas;

Art. 55 Deve ser divulgado amplamente, pelo(a) [Órgão ou Entidade], comunicados sobre ameaças e procedimentos que os usuários devem realizar ao detectar possíveis anormalidades nos ativos de informação.

Art. 56 É dever do(a) [Órgão ou Entidade] isolar o ambiente ou os ativos de informação suspeitos, infectados e os que podem ser potencialmente comprometidos para análise e identificação de malware.

Art. 57 O [Órgão ou Entidade] precisa investigar todo incidente onde haja suspeita de que a origem possa ser um malware, para verificar se essa é de fato a causa subjacente.

Art. 58 O(A) [Órgão ou Entidade] deve identificar quais ativos de informação estão infectados por malware, para que assim, todos estes ativos consigam ser analisados e, consequentemente, ações específicas de contenção, erradicação e recuperação sejam realizadas.

Art. 59 É dever do(a) [Órgão ou Entidade] garantir que toda a identificação de infecção por malware seja realizada por meio de ferramentas automatizadas.

Art. 60 É dever do(a) [Órgão ou Entidade] classificar e nomear cuidadosamente os seus ativos de informação, de forma a tornar a detecção de malware mais eficaz.

Art. 61 O(A) [Órgão ou Entidade] deve determinar quais tipos de informações de identificação do ativo de informação são necessárias (IP, Sistema Operacional, localização física do ativo de informação), bem como quais fontes de dados dos sistemas de detecção serão utilizadas.

Art. 62 O(A) [Órgão ou Entidade] deve utilizar ferramentas de detecção do malware como SIEM, IDS, IPS, para identificar as características de ação do malware.

Art. 63 O(A) [Órgão ou Entidade] deve pesquisar informações sobre malware em fornecedores de antivírus, tais como:

I. Categoria do malware (por exemplo, worm, trojan, vírus);

II. Serviços, portas, protocolos que são explorados pelo malware;

III. Como o malware impacta o ativo de informação infectado;

IV. Vulnerabilidades que são exploradas pelo malware;

V. Como o malware se propaga nos ativos de informação;

VI. Como realizar a contenção e remoção do malware.

Art. 64 O(A) [Órgão ou Entidade] pode utilizar sniffers de pacotes para realizar a busca ativa de um malware específico.

Art. 65 A equipe de segurança da informação do(a) [Órgão ou Entidade] deve analisar o comportamento do malware de forma ativa (ao executar o malware em um ambiente controlado) ou de forma forense (analisando as evidências de ações do malware no ativo de informação infectado).

Art. 66 Caso a análise de malware seja por meio de ambiente controlado, o(a) [Órgão ou Entidade] deve estabelecer um sistema de testes isolado, sem acesso à sua rede corporativa e operacional.

Art. 67 O sistema de testes deve ser estabelecido em um sistema operacional virtualizado do(a) [Órgão ou Entidade], que após a realização da análise de comportamento do malware, deverá ser apagado.

Art. 68 O sistema de testes deve incluir ferramentas de identificação e detecção de malware atualizadas.

Art. 69 O(A) [Órgão ou Entidade] pode utilizar da análise de logs para analisar o comportamento de um malware.

Art. 70 Implementar ferramenta de análise de tráfego baseado em rede, como o sistema de prevenção de intrusão, buscando pacotes suspeitos, fluxos incomuns na rede e assinaturas de ataque, visando interromper a atividade potencialmente maliciosa.

Art. 71 O(A) [Órgão ou Entidade] deve utilizar tecnologias de inspeção e filtragem de conteúdo, tais como as especificadas a seguir:

I. Ferramenta de filtragem de spam;

II. Ferramenta de filtragem e inspeção de conteúdo da web;

III. Listas negras de sites maliciosos.

IV. [Acrescentar outras tecnologias de inspeção e filtragem de conteúdo].

Art. 72 O(A) [Órgão ou Entidade] deve utilizar métodos de arquitetura defensiva, tais como:

I. Proteção de BIOS;

II. SandBox;

III. [Acrescentar métodos de arquitetura defensiva].

CAPÍTULO VII
REMEDIAÇÃO - CONTENÇÃO E ERRADICAÇÃO

A remediação de incidentes envolvendo malwares tem dois objetivos principais: impedir a propagação do malware e evitar maiores danos aos hosts. Quase todos os incidentes de malware exigem ações de contenção e erradicação. Ao abordar um incidente, é importante que o [Órgão ou Entidade] decida quais métodos de contenção e erradicação devem ser empregados no início da resposta.

Seção I
Da Contenção

Art. 73 As estratégias de contenção devem apoiar os responsáveis pelo tratamento de incidentes na seleção da combinação apropriada de métodos, com base nas características de uma situação específica.

Art. 74 Os usuários devem receber instruções sobre como identificar infecções e quais medidas tomar se um host for infectado, tais instruções incluem e não se limitam a:

I. Ligar para o suporte técnico;

II. Desconectar o host da rede;

III. Desligar o host.

IV. [Acrescentar instruções adequadas ao caso]

Art. 75 O malware identificado deve ser removido dos ativos do(a) [Órgão ou Entidade].

Art. 76 Softwares não autorizados devem ser removidos dos ativos do(a) [Órgão ou Entidade] ou receber uma exceção documentada.

Art. 77 Todas as exceções devem ser anotadas no inventário de software e no registro de exceções.

Art. 78 O(A) [Órgão ou Entidade] deve ter mecanismos alternativos para distribuir informações aos usuários, como enviar mensagens para todas as caixas de correio de voz do(a) [Órgão ou Entidade], afixar cartazes nas áreas de trabalho e distribuir instruções nas entradas dos edifícios e escritórios.

Art. 79 O(A) [Órgão ou Entidade] deve identificar e implementar métodos para fornecer utilitários e atualizações de software aos usuários que deverão ajudar na contenção.

Art. 80 É prudente que o(a) [Órgão ou Entidade] utilize tecnologias automatizadas para prevenir e detectar infecções, o que irá ajudar a conter muitos incidentes causados por malwares. Essas tecnologias incluem softwares, tais como antivírus, filtragem de conteúdo e prevenção de intrusões.

Art. 81 O(A) [Órgão ou Entidade] deve estar preparado para usar outras ferramentas de segurança para conter o malware até que as assinaturas antivírus possam realizar a contenção de forma eficaz.

Art. 82 Se o(a) [Órgão ou Entidade] receber assinaturas atualizadas, é prudente testá-las pelo menos antes da implantação, para garantir que a atualização em si não cause um impacto negativo.

Art. 83 O(A) [Órgão ou Entidade] pode adotar vários métodos de detecção automatizados que não sejam software antivírus, tais como os seguintes:

I. Filtragem de conteúdo;

II. Software IPS baseado em rede;

III. Lista negra executável;

IV. [Acrescentar mecanismos de detecção automatizados diferente de antivírus].

Art. 84 Manter lista das portas TCP e UDP utilizadas por cada serviço, para que possa suportar a desativação de serviços de rede.

Art. 85 Manter uma lista de dependências entre os principais serviços para que a equipe de resposta a incidentes esteja ciente deles ao tomarem decisões de contenção.

Art. 86 O(A) [Órgão ou Entidade] pode parar serviços que estiverem com vulnerabilidades e oferecer outros alternativos com funcionalidades semelhantes aos usuários.

Art. 87 O(A) [Equipe de Resposta a Incidentes ou equivalente] deve considerar bloquear todo o acesso ao host externo (por endereço IP ou nome de domínio, conforme apropriado), se os hosts infectados tentarem estabelecer conexões com um host externo para baixar malwares, como por exemplo rootkits.

Art. 88 Se hosts infectados tentarem espalhar um malware, o(a) [Órgão ou Entidade] poderá bloquear o tráfego de rede dos endereços IP dos hosts para controlar a situação enquanto os hosts infectados são fisicamente localizados e limpos.

Art. 89 O(A) [Órgão ou Entidade] deve projetar e implementar suas redes para tornar a contenção, através da perda de conectividade, mais fácil e menos perturbadora, isso poderá incluir:

I. Colocar servidores e estações de trabalho em sub-redes separadas;

II. Uso de redes locais virtuais (VLAN) separadas para hosts infectados;

III. [Acrescentar formas de implementar redes para facilitar o isolamento de máquinas infectadas].

Art. 90 O(A) [Equipe de Resposta a Incidentes ou equivalente] deve selecionar uma combinação de métodos de contenção que, provavelmente, serão eficazes na contenção do atual incidente, ao mesmo tempo em que limita os danos aos hosts e reduz o impacto que os métodos de contenção podem ter sobre outros hosts.

Art. 91 O(A) [Órgão ou Entidade] deve apoiar decisões de contenção sólidas, tendo políticas que estabeleçam claramente quem tem autoridade para tomar decisões importantes de contenção e sob que circunstâncias (por exemplo, desconectar sub-redes da Internet).

[Acrescentar diretrizes cabíveis para o processo de Contenção].

Seção II
Da Erradicação

Embora o objetivo principal da erradicação seja remover malware de hosts infectados, a erradicação normalmente envolve mais do que isso. Se uma infecção foi bem-sucedida devido a uma vulnerabilidade do host ou outra falha de segurança, como um compartilhamento de arquivo não seguro, a erradicação inclui a eliminação ou mitigação dessa fraqueza, o que pode impedir que o host seja reinfectado ou infectado por outra instância de malware ou uma variante da ameaça original.

Art. 92 Nos casos em que a destruição do malware é possível, as ferramentas mais comuns para erradicação que o(a) [Órgão ou Entidade] normalmente são: software antivírus, software de controle de acesso à rede e outras ferramentas projetadas para remover malware e corrigir vulnerabilidades.

Art. 93 O(A) [Órgão ou Entidade] pode utilizar métodos automatizados de erradicação, como acionar verificações de antivírus remotamente.

Art. 94 O(A) [Órgão ou Entidade] deve fornecer instruções e atualizações de software aos usuários além de assistência durante o processo de erradicação de malwares.

Art. 95 O(A) [Órgão ou Entidade] pode manter áreas de suporte técnico formais ou informais nas principais instalações para aumentar a eficácia e eficiência na erradicação de malwares.

Art. 96 Durante incidentes graves, integrantes da equipe de TI podem ser realocados temporariamente de outras funções para ajudar nos esforços de erradicação.

Art. 97 O(A) [Órgão ou Entidade] deve estar preparado para reconstruir hosts rapidamente, conforme necessário, quando ocorrerem incidentes de malware.

Art. 98 Em vez de realizar ações típicas de erradicação, o(a) [Órgão ou Entidade] deve reconstruir qualquer hospedeiro que apresente alguma das seguintes características de incidente:

I. Um ou mais invasores obtiveram acesso de nível de administrador ao host;

II. O acesso não autorizado de nível de administrador ao host estava disponível para qualquer pessoa através de um *backdoor*, através de um compartilhamento desprotegido criado por um *worm* ou por outros meios;

III. Os arquivos do sistema foram substituídos por um cavalo-de-tróia, *backdoor*, *rootkit*, ferramentas de ataque ou outros meios;

IV. O host fica instável ou não funciona corretamente depois que o malware foi erradicado por software antivírus ou outros programas ou técnicas. Isso indica que o malware não foi completamente erradicado ou que causou danos a arquivos ou configurações importantes do sistema ou de aplicativos;

V. Há dúvidas sobre a natureza e a extensão da infecção ou sobre qualquer acesso não autorizado obtido por causa da infecção.

Art. 99 A [Equipe de Resposta a Incidentes ou equivalente] deve realizar, periodicamente, atividades de identificação de hospedeiros que ainda estão infectados e estimar o sucesso da erradicação.

Art. 100 O(A) [Órgão ou Entidade] deve se esforçar para reduzir o número suspeito de máquinas infectadas e vulneráveis a níveis suficientemente baixos, para que, se todas elas estiverem conectadas a rede de uma só vez e todas as máquinas vulneráveis estiverem infectadas, o impacto geral das infecções seja o menor possível.

[Acrescentar diretrizes cabíveis para o processo de Erradicação].

CAPÍTULO VIII
DA RECUPERAÇÃO

Os dois principais aspectos da recuperação de incidentes de malware são restaurar a funcionalidade e os dados dos hosts infectados e remover medidas de contenção temporárias. Ações adicionais para restaurar hosts não são necessárias para a maioria dos incidentes de malware que causam danos limitados ao host.

Art. 101 O(A) [Órgão ou Entidade] deve observar dois aspectos principais da recuperação de incidentes de malware, que são:

Art. 102 Restaurar a funcionalidade e os dados dos hosts infectados; e

Art. 103 Remover medidas de contenção temporárias.

Art. 104 Para incidentes de malware que são muito mais prejudiciais, como cavalos de Tróia, rootkits ou backdoors, que corrompem milhares de arquivos de sistema e de dados ou destroem discos rígidos, muitas vezes é melhor reconstruir primeiro o host e depois proteger o host para que ele não fique mais vulnerável à ameaça de malware.

Art. 105 O(A) [Órgão ou Entidade] deve considerar cuidadosamente os possíveis cenários de pior caso, como uma nova ameaça de malware que exija a reconstrução de uma grande porcentagem de suas estações de trabalho, e determinar como os hosts seriam recuperados nesses casos, isto pode incluir:

I. Identificação de quem executaria as tarefas de recuperação;

II. Estimativa de quantas horas de trabalho seriam necessárias e quanto tempo de calendário decorreria;

III. Determinação de como os esforços de recuperação deveriam ser priorizados.

Art. 106 O(A) [Órgão ou Entidade] deve determinar quando remover medidas de contenção temporárias.

Art. 107 As equipes de resposta a incidentes devem esforçar-se para manter medidas de contenção em vigor até que o número estimado de hospedeiros infectados e de hospedeiros vulneráveis à infecção seja suficientemente baixo, de modo que os possíveis incidentes subsequentes tenham poucas consequências.

Art. 108 O(s) [responsáveis pelo tratamento de incidentes] também deve(m) considerar medidas de contenção alternativas que possam manter adequadamente a contenção do incidente e, ao mesmo tempo, causar menor impacto nas funções normais do(a) [Órgão ou Entidade].

Art. 109 A equipe de resposta a incidentes deve avaliar os riscos de restaurar o(s) serviço(s).

Art. 110 A [alta gestão] deve, em última análise, ser responsável por determinar o que deve ser feito, com base nas recomendações da equipe de resposta a incidentes e na compreensão da gestão sobre o impacto no(a) [Órgão ou Entidade] da manutenção das medidas de contenção.

[Acrescentar diretrizes cabíveis para o processo de Recuperação].

CAPÍTULO IX
RELATÓRIOS E LIÇÕES APRENDIDAS

Como o tratamento de grandes incidentes de malware pode ser extremamente caro, é particularmente importante que as organizações conduzam atividades robustas de relatórios e lições aprendidas para grandes incidentes de malware. Embora seja razoável dar aos encarregados algum tempo para colocarem em dia outras tarefas, as reuniões de revisão e outros esforços devem ocorrer rapidamente, enquanto o incidente ainda está fresco na mente de todos.

Art. 111 Todos os alertas de alta gravidade confirmados devem ser relatados ao [Responsável do Órgão ou Entidade].

Art. 112 Os usuários devem ser treinados para reportar malwares descobertos a [Unidade responsável por receber notificações sobre malwares no Órgão ou Entidade].

Art. 113 Possíveis resultados de atividades de lições aprendidas para incidentes de malware podem ser os seguintes:

I. Mudanças na política de segurança;
II. Mudanças no Programa de Conscientização;
III. Reconfiguração de software;
IV. Implantação de software de detecção de malware;
V. Reconfiguração do software de detecção de malware;
VI. [Acrescentar resultados possíveis da atividade de lições aprendidas].

CAPÍTULO IX
DISPOSIÇÕES FINAIS

Art. 114 Reforçar o compromisso do(a) [Órgão ou Entidade] com a segurança da informação, incluindo a proteção contra malware, destacando a importância de todas as pessoas envolvidas seguirem a política estabelecida.

Art. 115 Enfatizar a responsabilidade de cada colaborador em aderir às práticas de segurança da informação estabelecidas e relatar qualquer atividade suspeita o mais rápido possível.

Art. 116 Promover uma cultura de segurança da informação em todo(a) [Órgão ou Entidade], incentivando a colaboração e a comunicação aberta sobre ameaças de malware e melhores práticas de segurança.

Art. 117 Garantir o apoio contínuo da alta administração para a implementação e execução eficaz da Política de Defesas Contra Malware, alocando recursos adequados e priorizando a segurança cibernética como uma preocupação organizacional.

Art. 118 Avaliar periodicamente o impacto da Política de Defesas Contra Malware na segurança geral do(a) [Órgão ou Entidade], identificando áreas de sucesso e oportunidades de melhoria.

Art. 119 Considerar a comunicação da Política de Defesas Contra Malware para partes externas, como fornecedores e parceiros, para promover a conscientização e colaboração na proteção contra ameaças.

Art. 120 Integrar a Política de Defesas Contra Malware aos planos de continuidade do negócio, garantindo que o(a) [Órgão ou Entidade] se capacite para lidar com interrupções causadas por ataques de malware e outros incidentes de segurança da informação.

[Acrescentar as disposições finais que devem ser considerados para a política].

Não conformidade

Descrever claramente as consequências (legais e/ou disciplinares) do não cumprimento da política pelos colaboradores, incluindo terceiros. Pode ser pertinente descrever o processo de escalonamento para repetida não conformidade.

Ex.: Em caso de violação desta política poderão ser aplicadas sanções previstas na Lei 8.112/1990 e outras legislações cabíveis

As sanções por descumprimento podem incluir, mas não se limitam a um ou mais dos seguintes:

1. Processo Administrativo disciplinar de acordo com a legislação aplicável
2. Exoneração.
3. Ação judicial de acordo com as leis aplicáveis e acordos contratuais.

Concordância

Inclua uma seção que confirme o entendimento e o acordo para cumprir a política. Assinaturas e datas são necessárias. Uma declaração de amostra é fornecida abaixo.

Li e entendi a Política de Defesas Contra Malware do(a) [Órgão ou Entidade]. Entendo que caso venha a violar as diretrizes estabelecidas nesta Política, posso enfrentar ações legais ou disciplinares de acordo com as leis aplicáveis ou normas internas do(a) [Órgão ou Entidade].

Nome do Servidor/Empregado

Assinatura do Servidor/Data

ANEXO I

Este anexo tem a finalidade de fornecer os destaques das mudanças inseridas nas versões do Modelo de Política de Defesas contra Malware, em comparação com o documento originalmente publicado em maio de 2024.

Mudanças da Versão 1.1

As mudanças inseridas nesta versão em comparação com a anterior visam a adequação do Modelo com o Controle 12 do Guia do Framework de Privacidade e Segurança da Informação.

Destacam-se as seguintes alterações:

- Ajuste na Seção Declarações da política, item 4. Prevenção de Incidentes de Malware através da inclusão de três tópicos para dar ênfase as medidas 12.3 e 12.4.