Modelo de Política de Gestão de Ativos

PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO (PPSI)

Versão 2.3

Brasília, junho de 2024

MODELO DE POLÍTICA DE GESTÃO DE ATIVOS

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

Coordenador-Geral de Privacidade

COORDENAÇÃO-GERAL DE SEGURANÇA DA INFORMAÇÃO

Loriza Andrade Vaz de Melo

Coordenadora-Geral de Segurança da Informação

Equipe Técnica de Elaboração

Amaury C. da Silveira Junior

Eder Ferreira de Andrade

Francisco Magno Felix Nobre

Heráclito Ricardo Ferreira Gomes

Ivaldo Jeferson de Santana Castro

Yuri Arcanjo de Carvalho

Ramon Caldas

Guilherme Rufino Junior

Guilherme Mendonça Medeiros

Equipe Revisora

Marcus Paulo Barbosa Vasconcelos

Samuel Barichello Conceição

Sumaid Andrade de Albuquerque

Equipe Técnica de Revisão - Versão 2.3

Adriano de Andrade Moura

Anderson Souza de Araújo

Francisco Magno Felix Nobre

Ivaldo Jeferson de Santana Castro

Raphael César Estevão

Rogério Vinícius Matos Rocha

Histórico de Versões

Data	Versão	Descrição	Autor
31/03/2022	1.0	Modelo de Política de Gestão de Ativos	Equipe Técnica de Elaboração
05/05/2022	1.1	Modelo de Política de Gestão de Ativos	Equipe Técnica de Elaboração
31/03/2023	2.0	Atualização para alinhamento com o Guia do Framework de Privacidade e Segurança da Informação, conforme destacado no Anexo I.	Equipe Técnica de Revisão
06/07/2023	2.1	Atualização para alinhamento com o Guia Framework de Privacidade e Segurança da Informação, conforme destacado no Anexo I	Equipe Técnica de Revisão
11/10/2023	2.2	Atualização das diretrizes de Classificação de Nível de Acesso das Informações	Equipe Técnica de Revisão
18/06/2024	2.3	Atualização para alinhamento com as medidas 12.1, 12.2, 12.3, 12.4 e 12.5 do Controle 12 - Gestão da Infraestrutura de Rede - do Guia do Framework de Privacidade e Segurança da Informação, conforme destacado no Anexo I	Equipe Técnica de Revisão

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 Gestão de Ativos, 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 Gestão de Ativos 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 Gestão de Ativos no âmbito institucional.

Os Controles 1, 2 e 12 do Guia do Framework de Privacidade e Segurança da Informação (p. 36, 37 e 50) estabelecem que:

Controle 1: Inventário e Controle de Ativos Institucionais- *Gerenciar ativamente (inventariar, rastrear e corrigir) todos os ativos institucionais conectados à rede, com o objetivo de identificar precisamente quais necessitam ser monitorados e/ou protegidos dentro da empresa, mapeando todos os ativos não autorizados para uma possível remoção ou remediação futura.*

Controle 2: Inventário e Controle de Ativos de Software *- Gerenciar ativamente (inventariar, rastrear e corrigir) todo o software na rede para que apenas o software autorizado seja instalado e possa ser executado, e que todo o software não autorizado e não gerenciado seja encontrado e impedido de instalação ou execução.*

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 1, 2 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 1, 2 e 12 que estão contempladas por este Modelo são: 1.1, 1.2, 1.3, 1.4 ,1.5, 2.1, 2.2, 2.3, 2.4, 2.5, 2.6, 2.7, 12.1, 12.2, 12.3, 12.4 e 12.5.

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:

[1] < https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_framework_psi.pdf >. Acesso em 29/06/2023.

> *"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 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.

A gestão de ativos institucionais é o processo de aquisição, identificação, rastreamento, manutenção e descarte de um ativo de propriedade de uma empresa. A política de gestão de ativos fornece os processos e procedimentos para governar o ciclo de vida da gestão dos ativos institucionais enquanto uma instituição estiver usando um ativo. Um inventário deve ser criado e mantido para apoiar a missão da instituição. Este inventário deve ser atual e refletir os ativos atuais de propriedade e operados pela instituição.

Política de Gestão de Ativos

IMPORTANTE: Este modelo de Política de Gestão de Ativos 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 o a Gestão de Ativos, 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 exemplo 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, Política de Gestão de Riscos \ Política de Retenção de Dados \ 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 gestão de ativos. Além disso, afirmam os objetivos básicos da política e o que a política pretende alcançar.

Exemplo: O objetivo desta política é garantir que os ativos de informação sejam identificados adequadamente e que os controles de proteção recomendados para estes ativos de informação estejam em vigor.

Para manter a segurança e continuidade do negócio do [Órgão ou entidade], em sua missão é fundamental mapear e monitorar os ativos tecnológicos, para maior controle da organização, auxiliando na aplicação de atualizações, implementação de controles de segurança e gestão de risco da organização. Auxiliando também na recuperação de incidentes.

Os ativos de informação da (o) [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 “dono”, no qual realizará a classificação do ativo de informação e deverá ser registrado 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.

EX: Esta Política de Gestão de Ativos se aplica a todos os processos de negócios e dados, sistemas de informação e componentes, pessoal e áreas físicas de [inserir nome da empresa].

- Esta política se aplica a todos os ativos de informação no [Órgão ou entidade], incluindo ativos fora do [Órgão ou entidade] armazenados em um serviço de nuvem. Ativos de informação neste contexto, incluem [citar os dados considerados críticos para organização, ex.: Documentos, base de dados, contratos, documentação de sistemas, procedimentos, manuais, logs de sistemas, planos, guias, programas de computador, servidores, computadores, e-mail, arquivos pessoais e compartilhados, bancos de dados e conteúdo da web específicos].
- A classificação dos ativos de informação e o escopo desta política serão revisados [informar a periodicidade, ex.: anualmente].

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;

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	Secção
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 1, 2 e 12
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
Guias Operacionais SGD	Todos
Instrução Normativa Nº 01/GSI/PR, de 27 de maio de 2020	Art.12, Inciso IV, alínea d
Instrução Normativa Nº 03/GSI/PR, de 28 de maio de 2021	Capítulo II
Instrução Normativa Nº 04/GSI/PR, de 26 de março de 2020	Capítulo II
Instrução Normativa Nº 05/GSI/PR, de 30 de agosto de 2021	Anexo
Lei Nº 12.527/2011 – Lei de Acesso à Informação (LAI)	Em sua íntegra
Lei Nº 13.709/2018 – Lei Geral de Proteção de Dados	CAPÍTULO VII - Seção I – Art. 46, Seção II Art. 50
NIST SP 800-53 v4	AC-3, AC-4, AC-16, AC-20, CM-8, CM-9, MP-2, MP-3, PL-4, PM-5, PS-6, RA-2, SC-16
Norma ABNT NBR ISO/IEC 27001:2013 Tecnologia da informação - Técnicas de segurança – Sistemas de gestão de segurança da informação - Requisitos;	A.8 (A.8.1., A.8.2., A.8.3.)
Norma Complementar nº 20/IN01/DSIC/GSIPR, (Revisão 01) - Estabelece as Diretrizes de Segurança da Informação e Comunicações para Instituição do Processo de Tratamento da Informação nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.	
Portaria GSI/PR nº 93, de 18 de outubro de 2021	Em sua íntegra
Enterprise Asset Management Policy Template CIS v8	Em sua íntegra
Software Asset Management Policy Template CIS v8 - November 2022	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.

CAPÍTULO I

DOS PRINCÍPIOS GERAIS

Art. 1° A Política de Gestão de Ativos de informação deve estar alinhada com a Política de Segurança da Informação da *[organização]*.

Art. 2° A Política de Gestão de Ativos de informação deve estar alinhada com uma gestão de continuidade de negócios em nível organizacional.

Art. 3° O processo de mapeamento de ativos de informação deve estruturar e manter um registro de ativos de informação, destinados a subsidiar os processos de gestão de risco, de gestão de continuidade e de gestão de mudanças nos aspectos relativos à segurança da informação.

Art. 4° As rotinas de inventário e mapeamento de ativos de informação devem ser orientadas para a identificação dos ativos de informação da organização, a fim de manter o escopo da organização mapeado e documentado.

Art. 5° O processo de mapeamento de ativos de informação deve considerar, preliminarmente os objetivos estratégicos da organização, seus processos internos, os requisitos legais e sua estrutura organizacional.

Art. 6° O registro de ativos de informação resultante do processo de mapeamento de ativos de informação deverá conter: os responsáveis (proprietários e custodiantes) de cada ativo de informação; as informações básicas sobre os requisitos de segurança da informação de cada ativo de informação; os contêineres de cada ativo de informação; as interfaces de cada ativo de informação e as interdependências entre eles.

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

Art. 7° Os seguintes ativos de informação devem ser considerados no processo de mapeamento de ativos de informação:

I. Ativos físicos;
II. Bancos de dados;
III. Dispositivos móveis;
IV. Hardwares;
V. Mídias removíveis;
VI. Níveis de permissões;
VII. Serviços;
VIII. Softwares.

[Acrescentar dos ativos de informação que devem ser considerados no processo].

CAPÍTULO II
DAS DIRETRIZES

Art. 8° Informações ou ativos de informação de instalações de processamento de informações devem ser inventariados e documentados e esse registro deve ser mantido atualizado.

Art. 9° A organização deverá utilizar da segmentação de rede para organizar seus ativos de informação.

Art. 10. A organização deve implementar o controle de acessos e privilégios mínimos para a administração dos ativos de informação.

Art. 11. A organização deve implementar a centralização de autenticação, autorização e auditoria (AAA) para a administração de seus ativos de informação, principalmente os ativos que fazem parte da infraestrutura de rede da organização.

Art. 12. A categorização do inventário deve ser aprovada pelas partes apropriadas ou autoridade de autorização

Art. 13. A organização deve adotar e fazer cumprir os níveis mínimos de disponibilidade de seus ativos de informação.

Art. 14. A organização empregará o uso de mecanismos automatizados para identificar sistemas autorizados e não autorizados, incluindo hardware ou software.

Art. 15. A organização deve assegurar que os ativos de informação inventariados possuam contrato de suporte em vigor.

Art. 16. A organização empregará o uso de ferramentas de descoberta ativa e/ou passiva para identificar dispositivos conectados à rede da instituição e automaticamente atualizar o inventário de ativos.

Art. 17. A organização utilizará ferramentas de inventário de software, quando possível, em toda a organização para automatizar a descoberta e documentação do software instalado.

Art. 18. A organização assegurará que exista um processo semanal para lidar com ativos não autorizados.

Art. 19. A organização utilizará controles técnicos em todos os ativos para garantir que apenas software autorizado seja executado, sendo estes reavaliados semestralmente ou com mais frequência.

Art. 20. A organização utilizará controles técnicos para garantir que apenas bibliotecas e scripts autorizados, e assinados digitalmente tenham permissão para serem executados.

Art. 21. A organização utilizará de scripts e protocolos de segurança para o acesso e administração dos ativos de informação.

Art. 22. A organização deverá elaborar e manter diagramas e demais documentações da arquitetura de rede da organização. A revisão destas documentações deverá ser realizada de forma periódica ou quando ocorrerem mudanças significativas, que possam impactar tais artefatos.

Art. 23. A organização deverá garantir que a infraestrutura de rede da organização esteja atualizada. Deverá ser realizada uma revisão das versões de software de forma periódica, ou quando for identificada uma vulnerabilidade que eleve o risco da organização

Art. 24. O inventário também deverá incluir atualizações ou remoções dos softwares, bem como dos sistemas de informação.

Art. 25. As atualizações e novas versões de softwares devem ser avaliadas e aprovadas antes da instalação.

Art. 26. A organização utilizará ferramenta de gerenciamento de endereços IP - ex.: *Dynamic Host Configuration Protocol (DHCP)* - para atualizar o inventário de ativos da instituição.

Art. 27. Cada ativo de informação (por exemplo, desktops, laptops, servidores, tablets), quando aplicável, deve ter uma etiqueta afixada ao dispositivo com esse identificador.

Art. 28. Registre o identificador de ativos da informação juntamente com outras informações relevantes no inventário de TI. Isso inclui:

I. Identificador de ativos
II. Data da compra
III. Preço de compra
IV. Descrição do item
V. Fabricante
VI. Número do modelo
VII. Número de série
VIII. Nome do proprietário do ativo corporativo (por exemplo, administrador, usuário), função ou unidade de negócios, quando aplicável.
IX. Localização física do ativo da empresa, quando aplicável
X. Endereço físico (controle de acesso à mídia (MAC))
XI. Endereço de Protocolo de Internet (IP)
XII. Data de validade da garantia/vida útil
XIII. Qualquer informação de licenciamento relevante
XIV. No caso de softwares instalados na organização deve ser registrado no inventário informações como:
    a) Título do software;

b) Desenvolvedor ou editor de software;

c) Data de aquisição;

d) Data de instalação;

e) Duração do uso;

f) Finalidade comercial;

g) Lojas de aplicativos;

h) Versões;

i) Mecanismo de implantação;

j) Data de fim do suporte, se conhecida;

k) Qualquer informação de licenciamento relevante;

l) Data de descomissionamento.

[Acrescentar as diretrizes para guarda dos ativos de informação].

CAPÍTULO III
DAS RESPONSABILIDADES DO PROPRIETÁRIO DO PROCESSO

(RECOMENDA-SE A LEITURA AO ART. 9º DA IN GSI/PR Nº 3/2021)

Art. 29. Identificar potenciais ameaças aos ativos de informação;

Art. 30. Identificar vulnerabilidades dos ativos de informação;

Art. 31. Consolidar informações resultantes da análise do nível de segurança da informação de cada ativo de informação ou de grupos de ativos de informação em um relatório;

Art. 32. Avaliar os riscos dos ativos de informação ou do grupo de ativos de informação.

Art. 33. Indivíduos que requerem acesso aos sistemas de informação devem seguir o procedimento adequado para receber tal acesso, como descritos na política de controle de acesso e catalogadas no sistema de gestão de ativos.

Art. 34. Os processos em torno do gerenciamento de mudança e de configuração também serão estabelecidos e monitorados.

Art. 35. Todos os ativos de informação devem ser devolvidos após a rescisão do contrato de trabalho ou contrato.

[Acrescentar outras diretrizes cabíveis para o processo de acesso].

CAPÍTULO IV
CRITICIDADE DO ATIVO DE INFORMAÇÃO

Art. 36. A criticidade dos ativos de informação críticos da organização é determinada pelo:

I. Requisitos legais;

II. Nível básico de disponibilidade

III. Pelo valor financeiro;

IV. Pelo seu potencial de agregar valor ao negócio;

V. Por sua vida útil e

[outros critérios de risco ou fatores de criticidade].

CAPÍTULO V
CLASSIFICAÇÃO DE NÍVEL DE ACESSO DAS INFORMAÇÕES

Art. 37. Todos os ativos de informação devem ser classificados de acordo com seu nível de acesso, a fim de assegurar o direito fundamental de acesso à informação, bem como dispor sobre a devida restrição de acesso sobre informações sigilosas, conforme previsto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação - LAI) e demais normas aplicáveis.

Art. 38. As informações armazenadas, transmitidas, processadas ou que se encontram sob a guarda dos ativos de informação do *[Órgão ou entidade]*, independentemente de seu formato e suporte, devem ser classificadas segundo seu nível de acesso, de acordo com a legislação pertinente, sobretudo com as disposições da LAI, do Decreto nº 7.724, de 16 de maio de 2012, e orientações ou normas complementares editadas por órgãos competentes.

Art. 39. A classificação de nível de acesso das informações deve observar às diretrizes constantes na LAI, Decreto nº 7.724, de 16 de maio de 2012 e outros normativos complementares que abordam o assunto.

Art. 40. As informações devem ser classificadas conforme os seguintes níveis de acesso:

I. **Pública**, com acesso irrestrito e visível a todos os usuários, inclusive pelo público externo;

II. **Restrita**, quando se tratar de informação sigilosa não classificada em grau de sigilo, protegidas por demais hipóteses legais de restrição de acesso; e

III. **Sigilosa classificada em grau de sigilo**, nos termos do art. 23 da Lei nº 12.527/2011, subdividida nos graus ultrassecreto, secreto ou reservado.

Art. 41. Os ativos de informação serão rotulados e manuseados com base nos procedimentos apropriados de classificação de nível de acesso de informações usados pela organização.

[Acrescentar as diretrizes para classificação das informações].

CAPÍTULO VI
MANIPULAÇÃO DE MÍDIA

Art. 42. A mídia removível também deve ser gerenciada pelo mesmo procedimento de classificação de ativos de informação usado pela organização.

Art. 43. A mídia removível deve ser protegida contra acesso não autorizado e uso indevido durante o uso e em trânsito, e deve ser descartada com segurança, usando os procedimentos apropriados.

Art. 44. A mídia contendo informações confidenciais e internas do *[Órgão ou entidade]* devem ser protegidas contra acesso não autorizado, uso indevido, corrupção durante o transporte e, preferencialmente, com o uso de criptografia.

[Acrescentar as diretrizes para manipulação da mídia].

CAPÍTULO VII
USO ACEITÁVEL

Art. 45. Padrões ou diretrizes para o uso aceitável de ativos devem ser documentados para indicar o que os usuários dos ativos de informação podem ou não fazer.

Art. 46. Os seguintes itens devem ser cobertos nas diretrizes de uso aceitáveis:

I. Uso do computador e dos sistemas de informação;

II. Uso de softwares e dados;

III. Uso da Internet e e-mail;

IV. Uso do telefone;

V. Uso de equipamentos e materiais de escritório.

Art. 47. Como requisito de acesso ao ativo de informação e como componente do treinamento de conscientização de segurança, todos os usuários dos ativos de informação, sejam funcionários ou terceiros, serão obrigados a fornecer aceitação assinada das diretrizes de uso aceitáveis

[Acrescentar as diretrizes para uso aceitável de ativos de informação].

Procedimentos Relevantes

Considere criar documentos de procedimentos formais que reforcem e apoiem as determinações 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 reaprovada pela alta administração.

Não conformidade

Descrever claramente as consequências (legais e/ou disciplinares) para o não cumprimento da política dos funcionários. 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:

Exemplo:

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.

Eu li e entendi a Política de Gestão de Ativos do [órgão/empresa/fundação]. Entendo que se eu violar as diretrizes estabelecidas nesta Política, posso enfrentar ações legais ou disciplinares de acordo com as leis aplicáveis ou normas internas do [órgão/empresa/fundação].

Nome do Servidor/Empregado

_____

Assinatura do funcionário Data

ANEXO I

Este anexo tem a finalidade de fornecer os destaques das mudanças inseridas nesta versão do Modelo de Elaboração da Política de Gestão de Ativos.

Mudanças da Versão 2.3

A versão 2.3 da Política de Gestão de Ativos foi atualizada para alinhar-se com as medidas do controle 12 do Guia do Framework de Privacidade e Segurança da Informação. Destacam-se as seguintes alterações:

- Inclusão do controle 12 e respectivas medidas à Introdução;
- Inclusão de novas referências adicionando o controle 12 do Guia de Framework de Privacidade e Segurança da Informação e a Instrução Normativa Nº 04/GSI/PR;
- Inclusão de 8 novas diretrizes, na seção Declarações da Política, no tópico Diretrizes, visando contemplar de modo mais claro as medidas 12.1 a 12.5 que trata da gestão de infraestrutura de redes;
- Ajuste do tópico “Criticidade do ativo de informação” para adoção ao gerenciamento de infraestrutura de redes atendendo o controle 12 do Guia de Framework de Privacidade e Segurança da Informação.

Mudanças da Versão 2.2

Nesta versão, destacam-se as seguintes alterações:

- Ênfase na classificação do nível de acesso às informações de acordo com a Lei 12.527/2011 e demais normas aplicáveis;
- Destaque ao tratamento das informações independente de seu formato, considerando seu nível de acesso e alinhado às diretrizes da Lei 12.527/2011 (LAI) e do Decreto 7.724/2012;
- Inclusão de texto orientativo indicando classificação de acordo com os procedimentos internos do órgão, estabelecendo os níveis adequados de acesso público, restrito ou sigiloso classificado em grau de sigilo e;
- Inclusão de Novas Referências Legais.

As alterações listadas acima foram realizadas em atenção à colaboração dada pela ANATEL.

Mudanças da Versão 2.1

A versão 2.1 da Política de Gestão de Ativos foi atualizada para alinhar-se com as medidas do Guia do Framework de Privacidade e Segurança da Informação. As principais alterações incluem:

- Inclusão do Controle 2 do Guia do Framework na seção Introdução;
- Alteração do texto no parágrafo 2 da seção Política de Gestão de ativos, substituindo "controles emergenciais previstos no anexo 5" por "controles emergenciais destacados pelas orientações constantes da seção de introdução deste documento";

- Adição da referência ao documento "Software Asset Management Policy Template CIS v8 - November 2022" e inserção da referência ao Controle 2 do Guia do Framework na seção Referência Legal e Boas Práticas;

- Inclusão de novas diretrizes na seção Declarações da Política, visando contemplar as medidas 2.2 e 2.3 do Guia do Framework.

Mudanças da Versão 2.0

As mudanças inseridas nesta versão visam a adequação 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 de aviso preliminar e agradecimentos; e referência de que controle e medidas do Framework de Privacidade e Segurança da Informação são atendidos pelo Modelo de Elaboração da Política de Gestão de Ativos.

Na seção Referência Legal e Boas Práticas:

- Referenciado o documento Enterprise Asset Management Policy Template CIS v8.

Na seção Declarações da Política:

- Foram inseridas novas diretrizes.