Guia do Framework de Privacidade e Segurança da Informação

Programa de Privacidade e Segurança da Informação
PPSI 2.0

MINISTÉRIO DA
GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS

GOVERNO DO BRASIL
DO LADO DO POVO BRASILEIRO

Versão 1.2

Brasília, 30 de janeiro de 2026

GUIA DO FRAMEWORK DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

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

Marta Juvina de Medeiros

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

Adriano de Andrade Moura

Anderson Souza de Araújo

Leonard Keyzo Yamaoka Batista

Raphael César Estevão

Rejane Monique Brelaz Castro

Rogério Vinícius Matos Rocha

Thainan Cardoso Rezende

Equipe de Revisão

Ricardo Borges Almeida

Histórico de versões

Data	Versão	Descrição	Autor
21/11/2025	1.0	Elaboração do Guia do *Framework* de Privacidade e Segurança da Informação do PPSI 2.0	Equipe Técnica de Elaboração
20/01/2026	1.1	Análise e inclusão da IN GSI/PR nº 9/2026 como norma de referência	Equipe Técnica de Elaboração
30/01/2026	1.2	Ajuste do grupo de implementação associado à medida 8.4	Equipe Técnica de Elaboração

Sumário

Licença *Creative Commons*

[1] Disponível em: https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode.

1 Termos e definições

Os termos e definições a seguir foram traduzidos a partir do CIS *Controls Guide* v8.1 e adaptados ao contexto da Administração Pública federal, sendo adotados neste guia objetivando alinhamento entre os escopos de aplicação das medidas de segurança da informação [1]. Demais termos utilizados neste guia e respectivo *framework* podem ser encontrados na Portaria SGD/MGI nº 9.511, de 28 de outubro de 2025 ou no Glossário de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República (GSI/PR) aprovado pela Portaria GSI/PR nº 93, de 18 de outubro de 2021.

- **Ativos institucionais**: ativos com potencial de tratar dados, incluindo dispositivos de usuário final, dispositivos de rede, dispositivos da Internet das Coisas (*Internet of Things*, IoT) e não computacionais e servidores em ambientes virtuais, baseados em nuvem e físicos.
  - **Dispositivos de rede**: dispositivos eletrônicos essenciais para comunicação e interação entre dispositivos em uma rede de computadores. Incluem pontos de acesso sem fio, *firewalls*, *gateways*, roteadores e *switches*. Podem ser *hardware* físico, dispositivos virtuais ou baseados em nuvem.
  - **Dispositivos de usuário final**: ativos institucionais utilizados por agentes públicos de uma organização. Incluem *desktops*, estações de trabalho, assim como dispositivos portáteis e móveis, como *notebooks*, *smartphones* e *tablets*.
  - **Internet das Coisas (IoT) e dispositivos não computacionais**: dispositivos com sensores, *software* e outras tecnologias que podem conectar, armazenar e trocar dados com outros dispositivos e sistemas. A conexão com a internet pode ser intermitente, inexistente ou persistente. Exemplos incluem *smartwatches* e outros dispositivos vestíveis, impressoras, telas inteligentes, dispositivos para casa inteligente, alto-falantes, sistemas de controle industrial e sensores de segurança física.
  - **Servidores**: dispositivo ou sistema que fornece recursos, dados, serviços ou programas a outros dispositivos em uma rede local (*Local Area Network*, LAN) ou rede ampla (*Wide Area Network*, WAN). Servidores podem fornecer recursos e usá-los simultaneamente de outro sistema. Podem existir em *datacenters*, nuvens públicas, privadas ou híbridas, incluindo *containers* temporários ou *workloads serverless*. Exemplos incluem servidores *web*, servidores de aplicação, servidores de *e-mail* e servidores de arquivos.
- **Mídias removíveis**: qualquer tipo de dispositivo de armazenamento que pode ser removido de um computador enquanto o sistema está funcionando e permite movimentação de dados entre sistemas. Exemplos incluem CDs, DVDs, discos *blu-ray*, discos rígidos externos, cartões SD, *backups* em fita, disquetes e *drives* USB.
- **Soluções de *software***: conjuntos de dados e instruções usadas para direcionar um computador a realizar tarefas específicas. Soluções de *software* incluem sistemas operacionais e aplicações, ambos podendo incluir serviços, bibliotecas ou interfaces de programação de aplicações (APIs).

- **Aplicações**: programas ou grupos de programas que rodam sobre um sistema operacional hospedado em ativos institucionais. Exemplos: aplicação *web*, banco de dados, baseada em nuvem e móvel.
- **Sistemas operacionais**: soluções de *software* que executam em ativos institucionais para gerenciar *hardware* e recursos de *software*, fornecendo serviços comuns para programas. Exemplos: Windows, Ubuntu, MacOS, Android, z/OS.
  - **Serviços**: programas especializados que executam tarefas críticas definidas para o sistema operacional, frequentemente iniciados com o sistema, atuando em segundo plano e podendo ser iniciados e parados por usuários. Exemplos: gerenciamento de comunicações de rede, usuários, permissões de arquivos, segurança do sistema e interação com dispositivos.
  - **Biblioteca**: base de código pré-compilada e compartilhável que inclui classes, procedimentos, *scripts*, dados de configuração, usada para desenvolver programas e aplicações. Projetada para ajudar programadores e compiladores a construir e executar software eficientemente.
  - **Interface de Programação de Aplicação (*Application Programming Interface*, API)**: conjunto de regras e interfaces que permitem a interação padronizada entre componentes de *software*, facilitando o acesso e comunicação com recursos internos e externos.
- ***Firmware***: soluções *de software* armazenadas na memória não volátil do dispositivo, como ROM ou memória *flash*, que permitem comunicação entre diferentes tipos de *hardware* e sistema operacional. Geralmente atualizadas fora do processo de atualização do sistema operacional e aplicações da organização.

- **Dados:** conjunto de fatos que podem ser examinados, considerados e usados para tomada de decisão. Embora os dados possam ser físicos, o CIS *Controls* foca principalmente na proteção dos dados digitais armazenados, transferidos e processados por ativos institucionais.
  - **Dados críticos**: dados físicos ou digitais armazenados, processados ou geridos pela organização que devem ser mantidos privados, precisos, confiáveis e disponíveis. Caso publicizados, acessados por pessoas sem autorização ou destruídos indevidamente, podem causar danos à organização, seja por violação ou desrespeito a políticas, contratos ou regulamentos.
  - ***Log***: um *log* de eventos, ou simplesmente *log*, é uma coleção ordenada de registros de eventos. Termos como "*log* de dados", "*log* de atividades" e "arquivo de *log*" são frequentemente usados para se referir a "*log*". Os *logs* podem ser persistentes, como um arquivo armazenado em disco, ou podem ser transitórios, como um fluxo de registros de eventos fornecido a um signatário por meio de uma rede. Exemplos: *logs* de sistema operacional, detecção de *antimalware*, base de dados, aplicação, rede, *firewall*, servidor *web* ou controle de acesso. Existem dois tipos de *logs* que geralmente são tratados e frequentemente configurados de forma independente: *logs* de sistema e *logs* de auditoria.

        - ***Logs* de sistema**: normalmente fornecem eventos em nível de sistema que mostram, por exemplo, horários de início e fim de diversos processos do sistema, falhas, entre outros. Esses *logs* são nativos dos sistemas e exigem menos configuração para serem ativados.
        - ***Logs* de auditoria**: frequentemente incluem eventos em nível de usuário – como quando um usuário fez *login* ou acessou um arquivo – e requerem mais planejamento e esforço para serem configurados. Estes *logs* geralmente contêm registros de eventos relevantes para a segurança.
    - **Dados físicos**: dados armazenados em documentos físicos (ex: papel) ou mídias removíveis físicas (ex: *drives* USB, *backups* em fita).
- **Usuários:** agentes públicos, fornecedores terceirizados, contratados, prestadores de serviços, consultores ou qualquer pessoa autorizada a acessar ativos institucionais, incluindo contas de usuários, administradores e serviços.
    - **Prestadores de serviço**: entidades que oferecem plataformas, soluções de *software* e serviços a outras organizações. Exemplos: consultores de TI, provedores de serviço gerenciado (*Managed Service Provider*, MSP), plataformas de soluções de *software* como serviço e provedores de serviços em nuvem. Incluem prestadores terceirizados e fornecedores, pagos ou gratuitos.
    - **Contas de usuário**: identidade composta por credenciais (ex: nome de usuário, senha) que define um usuário em um sistema. Controla arquivos, pastas e recursos acessíveis e tarefas permitidas. Para este documento, refere-se a contas padrão com privilégios limitados para atividades gerais.
    - **Contas de administrador**: contas para usuários com privilégios elevados, usadas para gerenciar *aspectos* do computador, domínio ou infraestrutura de TI. Cada conta deve ser vinculada a um usuário único. Exemplos: contas *root*, administrador local, administrador de domínio, contas administrativas de rede ou dispositivos de segurança.
    - **Contas de serviço**: criadas especificamente para executar aplicações, serviços e tarefas automatizadas no sistema operacional. Podem existir somente para possuir dados e arquivos de configuração. Cada conta tem um dono responsável. Não devem ser usadas para computação geral.
- **Rede:** conjunto de dispositivos interconectados que troca dados. Rede é um conjunto mais amplo que infraestrutura e arquitetura de rede.
    - **Infraestrutura de rede**: conjunto de recursos que fornecem conectividade, gestão, operações de negócio e comunicação. Inclui *hardware*, soluções de *software*, sistemas e dispositivos físicos, virtuais e em nuvem, permitindo comunicação entre usuários, serviços, aplicações e processos.
    - **Arquitetura de rede**: desenho físico e lógico de uma rede, definindo organização, conexões entre dispositivos e soluções de *software*, e os dados transmitidos. Deve incluir diagramas da arquitetura de rede e de segurança.

- **Documentação:** políticas, normas, procedimentos, processos, planos, diagramas e outros materiais escritos, físicos ou digitais. Exemplos: métodos de governança, processos adotados pelos usuários ou diagramas da arquitetura de rede.
  - **Plano**: documento que implementa políticas e pode incluir grupos de políticas, normas, procedimentos e processos.
  - **Política**: declaração oficial de governança que define objetivos específicos de um programa.
  - **Processo**: conjunto de tarefas e atividades gerais para alcançar objetivos relacionados à segurança.
  - **Procedimento**: conjunto ordenado de etapas que deve ser seguido para cumprir uma tarefa específica, definindo a forma aprovada de agir em ambiente tecnológico e organizacional.

2 Introdução

O presente **Guia do *Framework* de Privacidade e Segurança da Informação** tem como objetivo fornecer informações de referência claras e abrangentes para apoiar e esclarecer os diversos aspectos relacionados à concepção, estruturação e implementação dos controles e medidas que compõem o *framework* do Programa de Privacidade e Segurança da Informação (PPSI 2.0), estabelecido pela Portaria SGD/MGI nº 9.511, de 28 de outubro de 2025. Este documento é o guia principal do *framework*, que integra uma série de guias operacionais elaborados pela SGD/MGI para fomentar a privacidade e a segurança da informação.

Este guia apresenta a importância de cada controle proposto no *framework*, incluindo diretrizes que auxiliam as organizações desde a gestão básica até a implementação operacional das medidas, promovendo a conformidade, a maturidade e a resiliência dos órgãos nos aspectos relacionados à privacidade e segurança da informação.

Busca-se, com este documento, orientar a identificação, o acompanhamento e o preenchimento das lacunas em privacidade e segurança da informação, alinhando práticas às exigências legais aplicáveis. Ressalta-se, contudo, que a adoção do *framework* não equivale necessariamente ao cumprimento integral da legislação brasileira vigente sobre privacidade e segurança da informação. Ainda assim, seguramente o *framework* constitui uma ferramenta valiosa para as organizações elevarem seu nível de conformidade e de maturidade nessas temáticas.

Conforme estabelecido na referida Portaria, este guia destina-se a órgãos e entidades da Administração Pública federal direta, autárquica e fundacional que possuem unidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP). Contudo, não há impedimentos para que outras instituições adotem este guia e o *framework*, buscando aprimorar suas práticas de privacidade e segurança da informação.

Os usuários da estrutura de controles do PPSI 2.0 devem consultar https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/framework-guias-e-modelos para garantir que estejam empregando as orientações mais atualizadas.

Este documento está organizado em capítulos que apresentam, inicialmente, os termos e definições fundamentais para o entendimento da temática, seguido de uma introdução que contextualiza o Programa de Privacidade e Segurança da Informação (PPSI 2.0). Em seguida, a fundamentação e estruturação do framework são detalhadas, explicando as bases técnicas e normativas que embasam sua concepção. A parte central do guia é composta pelos controles do framework organizados em segmentos, abrangendo desde a estruturação básica para governança, instrumentos fundamentais, até controles específicos de segurança da informação e privacidade. Cada controle inclui uma visão geral, sua importância, procedimentos recomendados, respectiva lista de medidas e referenciais normativos. O documento finaliza com considerações finais e referências técnicas e normativas para consulta.

3 Fundamentação e estruturação do *framework*

A elaboração do *framework* considerou a existência de modelos amplamente reconhecidos sobre privacidade e segurança da informação, tanto em abrangência internacional quanto nacional. Destacam-se, entre esses modelos, o *Secure Controls Framework* (SCF), que trata de forma nativa e integrada as temáticas de privacidade e segurança da informação, e normas consolidadas como as séries ABNT NBR ISO/IEC 27001:2023 e 27002:2023 e ISO/IEC 27701:2025 [2], [3], [4], [5]. Iniciativas como o CIS *Controls* e seu *Privacy Companion Guide*, assim como os *frameworks* desenvolvidos pelo *National Institute of Standards and Technology* (NIST) – especificamente o *Cybersecurity Framework* (CSF) e o NIST *Privacy Framework* – também figuram como referenciais de boas práticas, abrangendo privacidade e segurança da informação de modo holístico e complementar [1], [6], [7], [8].

Cabe salientar, entretanto, que muitos desses referenciais apresentam orientações amplas e não abordam detalhadamente as particularidades impostas pela legislação brasileira aplicável aos órgãos da Administração Pública federal direta, autárquica e fundacional, especialmente diante das exigências estabelecidas pela Lei Geral de Proteção de Dados Pessoais (LGPD) e das determinações emitidas pela ANPD (Agência Nacional de Proteção de Dados) e pelo GSI/PR. Além disso, destaca-se o desafio de prover uma metodologia de implementação que seja flexível e adaptável, considerando os diferentes níveis de maturidade em privacidade e segurança da informação existentes entre os diversos órgãos e entidades públicas do SISP.

Diante desse contexto, e fundamentado nas experiências e demandas observadas no âmbito do Programa de Privacidade e Segurança da Informação (PPSI 1.0), estabelecido pela Portaria SGD/MGI nº 852, de 28 de março de 2023, foi concebido o *framework* do PPSI 2.0.

No PPSI 2.0, o *framework* apresenta uma estrutura alinhada às necessidades prioritárias dos órgãos e entidades integrantes do SISP de modo a abarcar de forma integrada e abrangente os elementos essenciais nas temáticas de privacidade e segurança da informação, sendo organizado em três segmentos:

- Segmento base, desdobrado nos controles “**Estruturação básica para governança**” e “**Instrumentos fundamentais**”, visa estabelecer ações essenciais necessárias para impulsionar os demais segmentos.
    - Estruturação básica para governança: esse controle inclui os papéis essenciais para a condução da governança em privacidade e segurança da informação, tais como a alta administração, o gestor de segurança da informação, o encarregado pelo tratamento de dados pessoais, o gestor de Tecnologia da Informação e Comunicação (TIC) e o responsável pela gestão da integridade. Esses papéis são decisivos para o alinhamento estratégico, operacional e de responsabilização, garantindo o cumprimento das diretrizes e a efetividade das ações propostas no *framework*.
    - Instrumentos fundamentais: neste controle são englobados os principais processos, políticas e mecanismos que asseguram a implementação

estratégica da governança nas temáticas. Entre esses instrumentos, destacam-se o Programa de Governança em Privacidade (PGP), o Programa de Governança em Segurança da Informação (PGSI), as políticas institucionais e os processos de gestão da segurança da informação alinhados à Instrução Normativa nº 03 do GSI/PR [9].

- Segmento de segurança da informação, essencialmente fundamentado no CIS *Controls*, cujo escopo foi correlacionado a decretos, normas da SGD/MGI e do GSI/PR, garantindo aderência ao ambiente regulatório brasileiro – **controles de 1 a 18**.
- Segmento de privacidade, inteiramente concebido com base na Lei Geral de Proteção de Dados Pessoais (LGPD) e demais resoluções da ANPD, de modo a estruturar os controles para a conformidade no tratamento dos dados pessoais por órgãos públicos federais – **controles de 19 a 25**.

Cada uma dessas categorias será apresentada em detalhes nos capítulos seguintes, com a devida explicitação sobre a sua fundamentação e estruturação específica. Serão então apresentados os controles que compõem cada categoria, incluindo uma visão geral do controle, justificativa quanto a importância do controle, procedimentos e ferramentas para sua implementação, e a lista de medidas relacionadas.

4 Controles do segmento base

O segmento base constitui o alicerce para a efetividade do Programa, garantindo que as diretrizes estratégicas sejam traduzidas em responsabilidades claras e em instrumentos normativos consistentes.

No âmbito do PPSI 2.0, este segmento é organizado em dois controles complementares: (i) o controle de estrutura básica para governança e (ii) o controle de instrumentos fundamentais. O primeiro assegura a definição e a formalização dos papéis essenciais à condução da governança, ao passo que o segundo consolida os instrumentos institucionais que sustentam a implementação e a manutenção das práticas de privacidade e segurança da informação. Em conjunto, esses controles criam a base organizacional necessária para a conformidade legal, a responsabilização e a gestão contínua das ações do PPSI 2.0.

4.1 CONTROLE 0: Estruturação básica para governança

Visão geral

Este controle estabelece os papéis estruturantes da governança em privacidade e segurança da informação, destacando responsabilidades formais para a alta administração, gestores e responsáveis setoriais.

Por que este controle é crítico?

A governança em privacidade e segurança da informação depende da atuação de atores institucionais com funções bem delimitadas. A ausência de papéis claramente definidos pode gerar riscos de lacunas de atuação, sobreposição de funções e perda de efetividade da governança. Esse controle assegura alinhamento estratégico e operacional, além de garantir que a organização disponha de lideranças e agentes com atribuições definidas para conduzir as ações do PPSI. O controle visa garantir que a alta administração, gestores e responsáveis setoriais atuem de maneira articulada e responsiva às exigências legais e regulatórias.

Procedimentos e ferramentas

A implementação deste controle requer a formalização de atos normativos internos que instituam claramente os papéis relacionados à estrutura para governança em privacidade e segurança da informação. Para garantir clareza de responsabilidades e evitar sobreposições, recomenda-se a utilização de matrizes de responsabilidade, como o modelo RACI – Responsável, Aprovador, Consultado e Informado –, que definem os níveis de atuação de cada agente envolvido. Além disso, é necessário estabelecer canais de comunicação estruturados entre os papéis definidos, de forma a assegurar o fluxo contínuo de informações e a integração entre diferentes instâncias da organização. Por fim, a efetividade da estrutura básica de governança depende da implantação de mecanismos de reporte periódico à alta administração, permitindo acompanhamento, supervisão e tomada de decisão tempestiva.

Lista de medidas

ID	Título, descrição e normas de referência
0.1	**A alta administração do órgão estabelece, mantém, monitora e aprimora o sistema de gestão de riscos e controles internos relativos aos temas de privacidade e segurança da informação?**
	A alta administração deve estabelecer, manter, monitorar e aprimorar o sistema de gestão de riscos e controles internos com vistas à identificação, à avaliação, ao tratamento, ao monitoramento e à análise crítica dos riscos que possam impactar a implementação da estratégia e a consecução dos objetivos da organização no cumprimento da sua missão institucional (Decreto nº 9203/2017, art. 17), sem prejuízo das responsabilidades dos gestores dos processos organizacionais. Nesse contexto, os temas de privacidade e segurança da informação devem estar integrados ao sistema de gestão de riscos e aos controles internos. Ademais, conforme Acórdão 2387/2024 – Plenário TCU, a alta administração da organização deve liderar o processo de gestão de riscos decorrentes de ataques cibernético.
	Normas de referência: Decreto nº 9.203/2017, art. 17.
0.2	**O órgão nomeou gestor de tecnologia da informação e comunicação?**
	Designar formalmente agente público, e respectivo substituto, preferencialmente entre servidores públicos efetivos, empregados públicos ou militares, para exercer o cargo de Gestor de Tecnologia da Informação e Comunicação, conforme atribuições previstas no inciso IV do art. 4º da Portaria nº 778/2019 e em demais normas correlatas.
	Normas de referência: Portaria SGD/ME nº 778/2019.
0.3	**O órgão nomeou gestor de segurança da informação?**
	Designar formalmente servidor, e respectivo substituto, para exercer o encargo de Gestor de Segurança da Informação conforme atribuições previstas no art. 19 da IN nº 1/2020, do Gabinete de Segurança Institucional, da Presidência da República (GSI/PR) e demais normas correlatas.
	Normas de referência: Decreto nº 12.572/2025, art. 10, III; IN GSI/PR nº 1/2020, art. 16, I, e Capítulo VI, Seção I; IN GSI/PR nº 3/2021, art. 46.
0.4	**O órgão nomeou encarregado pelo tratamento de dados pessoais?**
	Designar formalmente servidor, e respectivo substituto, para exercer o encargo de Encarregado pelo Tratamento de Dados Pessoais, nos termos do art. 41, § 2º, da Lei nº 13.709/2018, das Resoluções ANPD nºs 15/2024 e 18/2024 e demais normas correlatas.
	Normas de referência: LGPD, arts. 23, III, e 41; Resolução CD/ANPD nº 18/2024, arts. 3º, 4º, 5º e 7º; IN SGD/ME nº 117, de 19 de novembro 2020.

0.5	O órgão nomeou o responsável setorial pela gestão da integridade?
Designar formalmente o responsável setorial pela gestão da integridade, nos termos do disposto no art. 5º, II do Decreto nº 11.529/2023.	
Normas de referência: Decreto nº 11.529/2023, art. 5º, II.	

0.6	O órgão instituiu Comitê de Segurança da Informação?
Instituir Comitê de Segurança da Informação ou estrutura equivalente para deliberar sobre os assuntos relativos à Política Nacional de Segurança da Informação e sobre normas de segurança da informação, contemplando demais atribuições do art. 20 da IN GSI/PR nº 1/2020.	
Normas de referência: IN GSI/PR nº 1/2020, art. 16, II, e Capítulo VI, Seção II; Decreto nº 12.572/2025, art. 10, II.	

0.7	O órgão instituiu Comitê de Proteção de Dados Pessoais?
Instituir Comitê de Proteção de Dados Pessoais ou estrutura equivalente para deliberar sobre os assuntos relativos à Lei Geral de Proteção de Dados Pessoais, resoluções da ANPD e demais normas sobre o tema.	
Normas de referência: LGPD, art. 50; Resolução CD/ANPD nº 18/2024, art. 10, V.	

0.8	O órgão instituiu Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR)?
Instituir e implementar a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR), composta, preferencialmente, por servidores públicos civis ocupantes de cargo efetivo ou militares, com capacitação técnica compatível com as atividades da equipe. Para cada membro da Equipe deverá ser designado um substituto. Elaborar o documento de constituição da ETIR conforme NC n° 05/IN01/DSIC/GSIPR, devidamente aprovado pela alta administração da organização, para regulamentar o funcionamento da equipe.	
Normas de referência: IN GSI/PR nº 1/2020, art. 15, IV; NC n° 05/IN01/DSIC/GSIPR.	

4.2 CONTROLE 0: Instrumentos fundamentais

Visão geral

O controle de instrumentos fundamentais reúne os programas, políticas e mecanismos indispensáveis para a operacionalização da governança em privacidade e segurança da informação. Ele traduz em instrumentos práticos e normativos os papéis definidos no controle de estruturação básica para governança.

Por que este controle é crítico?

Mesmo com papéis bem definidos, a governança não se concretiza sem instrumentos formais que deem sustentação às práticas institucionais. Este controle garante coerência, padronização e conformidade dos processos, permitindo que o PPSI seja aplicado de forma uniforme em toda a organização.

Procedimentos e ferramentas

A adoção deste controle pressupõe a elaboração, aprovação e publicação formal dos instrumentos de privacidade e segurança da informação, assegurando que sejam submetidos a revisões periódicas para manutenção de sua atualidade e aderência legal. Esses documentos devem ser disponibilizados de maneira acessível a todos os agentes públicos ou partes interessadas, de modo a garantir conhecimento institucional e aplicação uniforme. É igualmente relevante promover a integração entre os programas de privacidade e de segurança da informação, de forma que atuem de maneira coordenada e complementar. Além disso, a adoção de processos estruturados de gestão de risco e de conformidade fortalece a base de governança, enquanto o monitoramento contínuo da aplicação dos instrumentos garante sua efetividade. Por fim, recomenda-se que os processos institucionais de privacidade e segurança da informação sejam incorporados às avaliações internas, de modo a verificar a conformidade e melhorar a eficácia dos processos.

Lista de medidas

ID	Título, descrição e normas de referência
0.9	**O órgão possui Programa de Governança em Segurança da Informação (PGSI)?**
Instituir e implementar, preferencialmente em instância colegiada, o PGSI, documento que contém, no mínimo, o disposto na IN GSI/PR nº 3/2021, art. 45, na forma de ações estruturadas, políticas, normas e procedimentos para promover a segurança da informação na organização. Recomenda-se que o PGSI contemple papéis e responsabilidades dos agentes públicos envolvidos em sua execução, os prazos para realização das ações, além da programação para implementação dos controles e medidas de segurança da informação do PPSI, e que especifique indicadores de desempenho, como o iSeg, a serem medidos ao longo da execução do Programa. Revisar e atualizar o PGSI com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas de suas ações.	
Normas de referência: IN GSI/PR nº 1/2020, art. 19, I, V, XI, IN GSI/PR nº 3/2021, art. 45.	
0.10	**O órgão possui Programa de Governança em Privacidade (PGP)?**
Instituir e implementar, preferencialmente em instância colegiada, o PGP, documento que contém, no mínimo, o disposto na Lei nº 13.709/2018, art. 50, §2°, I, na forma de ações estruturadas, políticas, normas e procedimentos para o tratamento de dados pessoais pela organização. Recomenda-se que o PGP contemple papéis e responsabilidades dos agentes públicos envolvidos em sua execução, os prazos para realização das ações, além da	

programação para implementação dos controles e medidas de privacidade e proteção de dados pessoais do PPSI, e que especifique indicadores de desempenho, como o iPriv, a serem medidos ao longo da execução do Programa. Revisar e atualizar o PGP com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas de suas ações.

Normas de referência: Lei nº 13.709/2018, art. 50.

0.11 O órgão possui Política de Segurança da Informação (POSIN)?

Instituir e implementar uma Política de Segurança da Informação (POSIN), a partir da formalização e aprovação por parte da autoridade máxima da instituição, com o objetivo de estabelecer diretrizes, responsabilidades, competências e subsídios para a gestão da segurança da informação. Revisar e atualizar a POSIN periodicamente ou quando ocorrerem mudanças significativas na organização que possam impactar esta medida.

Normas de referência: IN GSI/PR nº 1/2020, Capítulo III, art. 19, III; Decreto nº 12.572/2025, art. 10, IV.

0.12 O órgão possui Política de Proteção de Dados Pessoais?

Instituir e implementar uma Política de Proteção de Dados Pessoais, que estabeleça as diretrizes para o tratamento de dados pessoais, independentemente do meio em que são tratados, incluindo papéis e responsabilidades dos agentes públicos envolvidos nos tratamentos de dados pessoais. Instituir e divulgar demais políticas, normas e procedimentos sobre a temática. Revisar e atualizar os documentos periodicamente ou quando ocorrerem mudanças significativas na organização que possam impactar esta medida.

Normas de referência: Lei nº 13.709/2018, art. 50.

0.13 O órgão possui um processo de gestão de riscos de segurança da informação?

Estabelecer e manter, em conformidade ao Capítulo III da IN GSI/PR nº 3/2021, um processo de gestão de riscos de segurança da informação alinhado com o modelo de gestão de riscos institucional, compatível com a missão e os objetivos estratégicos da organização considerando o disposto nos incisos do art. 11. Além disso, o processo deve ser composto por, no mínimo: plano de gestão de riscos de segurança da informação, conforme disposto no art. 13; relatório de identificação, análise e avaliação dos riscos de segurança da informação, conforme disposto no art. 14; e, relatório de tratamento de riscos de segurança da informação, conforme disposto no art. 15. Considerar as atribuições dispostas nos arts. 16 e 17.

Normas de referência: IN GSI/PR nº 1/2020, art. 19, IV; IN GSI/PR nº 3/2021, Capítulo III; Decreto nº 12.572/2025, art. 3º, VI, e art. 4º, III.

0.14 O órgão possui um processo de gestão de continuidade de negócios em segurança da informação?

Estabelecer e manter, em conformidade ao Capítulo IV da IN GSI/PR nº 3/2021, um processo de gestão de continuidade de negócios em segurança da informação baseado nas estratégias de continuidade para as atividades críticas, na avaliação dos riscos levantados no processo de gestão de riscos e nas diretrizes institucionais sobre gestão de continuidade de negócio. Tal processo deve ser composto por um plano de continuidade de negócios em segurança da informação, o qual observará o disposto no relatório de identificação, análise e avaliação de riscos de segurança da informação e a prioridade de recuperação dos processos de negócio, revisado uma vez por ano ou após mudanças significativas nos itens que compõem o plano. Além disso, o conteúdo do plano deve incluir o disposto no art. 23, e ser testado regularmente. Considerar as atribuições dispostas nos arts. 25, 26 e 27.

Normas de referência: IN GSI/PR nº 3/2021, Capítulo IV.

0.15 O órgão possui um processo de gestão de mudanças dos aspectos de segurança da informação?

Estabelecer e manter, em conformidade ao Capítulo V da IN GSI/PR nº 3/2021, um processo de gestão de mudanças nos aspectos de segurança da informação, respaldado nos relatórios do processo de gestão de riscos em segurança da informação e considerando a análise crítica das consequências de mudanças não previstas, atuando em ações para amenizar os efeitos adversos. O processo deve prever que a mudança seja classificada em emergencial, rotineira ou proativa, nos termos do art. 29. O processo deve ser constituído, minimamente, dos documentos de descrição da mudança e de avaliação e aprovação da mudança, contemplando o conteúdo dos arts. 32 e 34. Considerar as atribuições dispostas no parágrafo único do art. 31 e nos arts. 35 e 36.

Normas de referência: IN GSI/PR nº 3/2021, Capítulo V.

0.16 O órgão possui um processo de avaliação de conformidade dos aspectos de segurança da informação?

Estabelecer e manter, em conformidade ao Capítulo VI da IN GSI/PR nº 3/2021, um processo de avaliação de conformidade nos aspectos de segurança da informação. O processo deve ser constituído, minimamente, do plano de verificação de conformidade e do relatório de avaliação de conformidade, contemplando o conteúdo do art. 39 e art. 40. Considerar as atribuições dispostas nos arts. 41, 42 e 43.

Normas de referência: IN GSI/PR nº 1/2020, art. 19, VIII; IN GSI/PR nº 3/2021, Capítulo VI; Decreto nº 12.572/2025, art. 10, VI.

0.17 O órgão possui processo de gestão de riscos relacionados ao tratamento de dados pessoais?

Estabelecer e manter um processo documentado de gestão de riscos relacionados às operações de tratamento de dados pessoais, independentemente do meio em que ocorrem, que considere também a etapa de aplicação de medidas de segurança, técnicas e

administrativas, testadas e avaliadas, aptas a proteger os dados pessoais. Periodicamente, realizar revisão ou atualização deste processo, assim como em casos específicos quando ocorrerem mudanças que impactem de forma significativa esta medida. Este processo pode ser incorporado a outros processos institucionais de gestão de riscos da organização.
Normas de referência: Lei nº 13.709/2018, arts. 38, 44 e 50; Decreto nº 12.572/2025, art. 3º, VI, e art. 4º, III.

5 Controles do segmento de segurança da informação

Os controles e medidas de segurança da informação propostos neste *framework* foram embasados no CIS *Controls*® v8.1, formalmente conhecido como CIS *Critical Security Controls*®, o qual consiste de um conjunto recomendado de melhores práticas priorizadas de defesa cibernética [1]. Elas fornecem ações específicas e práticas de proteção contra os ataques mais difundidos e críticos da atualidade.

Conforme descrito no CIS *Controls Guide* v8.1, as medidas de segurança estabelecidas no CIS *Controls* refletem o conhecimento combinado de especialistas de todas as partes do ecossistema, com diferentes papéis (analistas de ameaças, profissionais de tecnologia da informação, equipes de resposta a incidentes, gestores de vulnerabilidades, provedores de soluções, usuários, formuladores de políticas, auditores, entre outros) e de vários setores (governo, energia, defesa, finanças, transporte, academia, consultoria, segurança, TI, entre outros), que se uniram para criar, adotar e apoiar o CIS *Controls*.

O CIS *Controls* é composto por um conjunto de 153 medidas, que são divididas em 18 controles e categorizadas em três Grupos de Implementação (GIs). As medidas visam a mitigação das vulnerabilidades dos mais comuns aos mais avançados tipos de ataque. Dessa forma, objetivando criar uma estratégia de priorização de medidas, o CIS elaborou uma metodologia de implementação das medidas com base nos referidos GIs. De modo resumido:

- o primeiro grupo (GI1), também conhecido como higiene cibernética, formado por 56 medidas básicas, foi concebido para instituições de pequeno a médio porte, com limitação no corpo de profissionais de TI e na experiência em segurança da informação;
- o segundo grupo (GI2) acomoda as instituições que empregam responsáveis por gerenciar e proteger a infraestrutura de TI. Inclui o GI1 e mais 74 medidas;
- por fim, o terceiro grupo (GI3) abrange as instituições que empregam especialistas nas diferentes facetas da segurança da informação. Inclui o GI1 e o GI2, mais 23 medidas.

Tendo em vista a maturidade do CIS *Controls*, ampla adoção pela comunidade de profissionais de segurança da informação, implementação por diferentes setores, abordagem consolidada na concepção e revisão de medidas, bem como a sua estratégia de implementação priorizada, o CIS *Controls* foi integralmente adotado no *framework* do PPSI 2.0. Ajustes pontuais, no entanto, foram realizados na descrição das medidas a fim de promover um maior alinhamento quanto ao termos utilizados na legislação e literatura brasileiras.

Adicionalmente, foi realizado um esforço de mapeamento das medidas do CIS *Controls* para a legislação brasileira, incluindo especialmente uma correlação com decretos, normas da SGD/MGI e do GSI/PR. Como consequência, observa-se que medidas dos diferentes GIs devem ser analisadas quanto à sua conformidade legal.

Destaca-se que a adoção de medidas não obrigatórias deve ser pautada pela gestão de riscos, considerando a análise de impacto e a probabilidade de vulnerabilidades e ameaças. Cabe à

organização avaliar criteriosamente a necessidade e o nível de implementação dessas medidas complementares, garantindo assim um *framework* com equilíbrio entre medidas essenciais obrigatórias e a flexibilidade para ajustar controles adicionais conforme o contexto e os riscos identificados.

Por fim, com a crescente adoção da computação em nuvem pela Administração Pública federal, é fundamental assegurar que os controles de segurança sejam interpretados à luz das particularidades e responsabilidades compartilhadas entre os órgãos e entidades do SISP e os provedores de serviços de nuvem, conforme os diferentes modelos de serviço em nuvem. Dessa forma, e no contexto do *framework* do PPSI 2.0, foi elaborado o Guia Complementar do *Framework* de Privacidade e Segurança da Informação para Computação em Nuvem, o qual manteve o alinhamento com CIS *Cloud Companion Guide* para direcionar a adaptação e implementação dos controles do CIS nos cenários específicos de computação em nuvem [10].

A seguir, são apresentados os controles de segurança da informação, incluindo a visão geral, importância do controle, procedimentos e ferramentas para sua implementação, e a lista de medidas relacionadas junto ao seu GI. Tais informações foram especialmente extraídas do CIS *Controls Guide* v8.1, resumidas e consolidadas neste capítulo.

5.1 CONTROLE 1: Inventário de ativos institucionais

Visão geral

Gerenciar ativamente (inventariar, rastrear e corrigir) todos os ativos institucionais (dispositivos de usuário final, incluindo portáteis e móveis; dispositivos de rede; dispositivos não computacionais/IoT e servidores) conectados à infraestrutura fisicamente, virtualmente ou remotamente e aqueles dentro de ambientes de nuvem, para conhecer com precisão a totalidade dos ativos que precisam ser monitorados e protegidos na organização. Isso também ajudará a identificar ativos não autorizados e não gerenciados objetivando remoção ou remediação.

Por que esse controle é crítico?

A organização não pode defender o que não sabe que possui. O controle gerenciado de todos os ativos institucionais também desempenha um papel crítico no monitoramento de segurança, resposta a incidentes, *backup* e recuperação de sistemas. As organizações devem saber quais dados são críticos para elas, e o gerenciamento adequado de ativos institucionais ajudará a identificar quais contêm ou gerenciam esses dados críticos, para que os controles de segurança apropriados possam ser aplicados.

Ativos adicionais que se conectam à rede da organização (por exemplo, sistemas de demonstração, sistemas de teste temporários, redes de convidados) devem ser identificados e/ou isolados para evitar que o acesso adversário afete a segurança das operações da organização.

Além disso, dispositivos portáteis de usuários finais se conectam periodicamente à rede e depois desaparecem, tornando o inventário de ativos desafiador neste cenário dinâmico. Da mesma forma, ambientes de nuvem e máquinas virtuais podem ser difíceis de rastrear em inventários de ativos quando estão desligados ou pausados. Manter uma visão atualizada e precisa dos ativos é um processo contínuo e dinâmico.

Procedimentos e ferramentas

Este controle requer ações técnicas e procedimentais, unidas em uma estratégia para promover o gerenciamento do inventário de ativos institucionais. Para auxiliar na implementação deste controle, as organizações podem aproveitar ferramentas de segurança já instaladas em ativos institucionais ou usadas na rede, incluindo tecnologias para varredura de descoberta da rede com um *scanner* de vulnerabilidades, revisar *logs antimalware*, *logs* de portais de segurança de *endpoint*, *logs* de rede de *switches* ou *logs* de autenticação e gerenciar os resultados em uma planilha ou banco de dados. Mesmo para pequenas organizações, raramente há uma única fonte para realizar o inventário de ativos institucionais, pois nem sempre os ativos são provisionados pelo departamento de TI. A realidade é que diversas fontes precisam ser consideradas para se ter um inventário de alta confiabilidade.

Organizações mais complexas podem adotar produtos mais abrangentes e de larga escala. Além das fontes de ativos mencionadas acima para pequenas organizações, as maiores podem coletar dados de portais e *logs* em nuvem de plataformas organizacionais, como: *Active Directory* (AD), *Single Sign-On* (SSO), Autenticação Multifator (MFA), Rede Privada Virtual (VPN), Sistemas de Detecção de Intrusão (IDS) ou Inspeção Profunda de Pacotes (DPI), Gerenciamento de Dispositivos Móveis (MDM) e ferramentas de varredura de vulnerabilidades. Existem ferramentas e métodos que normalizam esses dados para identificar dispositivos que são únicos entre essas fontes.

As referências a seguir apresentam informações detalhadas que fundamentam e auxiliam o processo de implementação deste controle conforme o ambiente computacional:

- Guia Complementar de Segurança da Informação para Computação em Nuvem: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi-2.0/
- Guias complementares do CIS *Controls* para dispositivos móveis, para internet das coisas e para sistemas de controle industrial, disponíveis em: https://www.cisecurity.org/controls/resources?crc=environment-specific-guidance

Lista de medidas

ID	Título, descrição e normas de referência	GI
1.1	**O órgão estabelece e mantém um inventário detalhado de ativos institucionais?**	GI1
Estabelecer e manter um inventário preciso e detalhado de todos os ativos institucionais que realizam tratamento de dados, incluindo: dispositivos de usuário final (incluindo portáteis e		

móveis), de rede, de Internet das Coisas, não computacionais e servidores, em adição ao disposto no Capítulo II da IN GSI/PR nº 3/2021. O inventário deve conter, no mínimo: endereço de rede (se estático), endereço de hardware, nome do ativo, proprietário, unidade organizacional, indicação se o ativo foi aprovado para se conectar à rede. Este inventário deve incluir ativos conectados à infraestrutura fisicamente, virtualmente ou remotamente e aqueles dentro de ambientes de nuvem. Também deve contemplar ativos regularmente conectados à infraestrutura de rede da organização, mesmo que não estejam sob seu controle. Revisar e atualizar o inventário semestralmente ou com mais frequência.

Normas de referência: IN GSI/PR nº 3/2021, Capítulo II.

1.2	**O órgão trata ativos institucionais não autorizados?**	**GI1**

Estabelecer e manter um processo para lidar com ativos institucionais não autorizados, optando por removê-los da rede, negar sua conexão remota ou colocá-los em quarentena.

Normas de referência: não identificada.

1.3	**O órgão usa ferramenta de descoberta ativa para identificação de ativos institucionais?**	**GI2**

Identificar os ativos institucionais conectados à rede da organização por meio de uma ferramenta de descoberta ativa, configurada para execução diária ou em intervalos menores.

Normas de referência: não identificada.

1.4	**O órgão usa o protocolo de configuração dinâmica de host (*Dynamic Host Configuration Protocol*, DHCP) para atualizar o inventário de ativos institucionais?**	**GI2**

Utilizar os registros (*logs*) de todos os servidores DHCP ou ferramentas de gerenciamento de endereços IP para atualizar o inventário de ativos institucionais.

Normas de referência: não identificada.

1.5	**O órgão usa ferramenta de descoberta passiva para identificação de ativos institucionais?**	**GI3**

Utilizar uma ferramenta de descoberta passiva para identificar ativos institucionais conectados à rede da organização. Revisar as varreduras e atualizar o inventário de ativos institucionais pelo menos semanalmente ou em intervalos menores, se necessário.

Normas de referência: não identificada.

5.2 CONTROLE 2: Inventário de soluções de *software*

Visão geral

Gerenciar ativamente (inventariar, rastrear e corrigir) todas as soluções de *software* na rede para que somente as autorizadas sejam instaladas e possam ser executadas, e que as não

autorizadas ou não gerenciadas sejam encontradas e impedidas de serem instaladas ou executadas.

Por que esse controle é crítico?

Um inventário completo de soluções de *software* é fundamental para prevenir ataques, pois permite identificar versões vulneráveis que invasores podem explorar remotamente, como por meio de navegadores desatualizados. Os invasores também podem usar esse acesso para se movimentar lateralmente pela rede. Sem esse inventário, a organização não sabe quais softwares são vulneráveis ou se há violações de licenciamento. Mesmo sem correções disponíveis, a lista permite adotar medidas temporárias de proteção contra ataques conhecidos e “explorações de dia zero”. Além disso, o inventário ajuda a eliminar softwares desnecessários que representam riscos à segurança. Assim, é essencial gerenciar todas as soluções de *software* na infraestrutura da organização para reduzir vulnerabilidades e proteger o ambiente.

Procedimentos e ferramentas

Listas de soluções de *software* permitidas podem ser implementadas por meio de ferramentas comerciais, políticas e recursos nativos em sistemas operacionais e suítes de segurança de *endpoints*. Ferramentas de inventário verificam soluções de *software* comuns e seus *patches*, usando padrões como *Common Platform Enumeration* (CPE). Soluções modernas combinam *antimalware*, *firewall*, IDS/IPS e controle por listas de permissões, que analisam nome, localização e *hash* de executáveis para permitir ou bloquear sua execução. Ferramentas avançadas permitem personalizar listas e definir regras específicas para usuários e horários, oferecendo controle detalhado sobre a solução de *software* em uso.

As referências abaixo contêm informações detalhadas para apoio à implementação deste controle:

- Guia Complementar de Segurança da Informação para Computação em Nuvem: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi-2.0/
- Guias complementares do CIS *Controls* para dispositivos móveis, para internet das coisas e para sistemas de controle industrial, disponíveis em: https://www.cisecurity.org/controls/resources?crc=environment-specific-guidance

Lista de medidas

ID	Título, descrição e normas de referência	GI
2.1	**O órgão estabelece e mantém um inventário de soluções de software?**	GI1
Estabelecer e manter um inventário detalhado de todas as soluções de software licenciadas instaladas em ativos institucionais, em adição ao disposto no Capítulo II da IN GSI/PR nº 3/2021. Revisar e atualizar o inventário semestralmente ou com mais frequência.		
Normas de referência: IN GSI/PR nº 3/2021, Capítulo II.		

2.2	**O órgão mantém em seu ambiente computacional apenas soluções de software suportadas pelos seus fornecedores?**	GI1

Assegurar que apenas soluções de software atualmente suportadas por seus fornecedores sejam categorizadas como autorizadas no inventário de soluções de software da organização. Se uma solução de software não for suportada, mas ainda assim necessária para o cumprimento da missão da organização, deve-se documentar uma exceção detalhando os controles compensatórios e a aceitação do risco residual. Para qualquer solução de software sem suporte que não possua documentação de exceção, a mesma deve ser categorizada como não autorizada. Revisar a lista de soluções de software suportadas mensalmente, ou em intervalos menores.

Normas de referência: não identificada.

2.3	**O órgão trata o uso de soluções de software não autorizadas?**	GI1

Assegurar que as soluções de software não autorizadas sejam removidas dos ativos institucionais ou recebam uma exceção documentada. Revisar semestralmente ou em intervalos menores.

Normas de referência: não identificada.

2.4	**O órgão utiliza ferramentas automatizadas de inventário de soluções de software?**	GI2

Utilizar ferramentas de inventário de soluções de software, quando possível, para automatizar a descoberta e documentação de soluções de software instaladas em toda a organização.

Normas de referência: não identificada.

2.5	**O órgão possui uma lista de soluções de software autorizadas?**	GI2

Elaborar lista de soluções de software autorizadas e implementar controles técnicos em todos os ativos para garantir que apenas estas soluções sejam executadas. Reavaliar a lista semestralmente ou em intervalos menores.

Normas de referência: não identificada.

2.6	**O órgão possui uma lista de bibliotecas de software autorizadas?**	GI2

Elaborar lista de bibliotecas de software autorizadas e implementar controles técnicos para assegurar que apenas bibliotecas autorizadas (tais como *.dll, *.ocx, *.so, etc) tenham permissão para serem carregadas nos processos em execução. Impedir que bibliotecas não autorizadas sejam carregadas nos processos. Reavaliar a lista semestralmente ou em intervalos menores.

Normas de referência: não identificada.

2.7	**O órgão possui uma lista de scripts autorizados?**	GI3

Elaborar lista de scripts autorizados e implementar controles técnicos, como assinaturas digitais e controle de versão, para assegurar que apenas scripts autorizados e assinados digitalmente (a exemplo de *.ps1, *.py e macros) tenham permissão para serem executados. Bloquear a execução de scripts não autorizados. Reavaliar a lista semestralmente ou em intervalos menores.
Normas de referência: não identificada.

5.3 CONTROLE 3: Proteção de dados

Visão geral

Aplicar processos e controles técnicos para identificar, categorizar, utilizar, reter e descartar dados com segurança, garantindo a proteção dos dados ao longo de todo o seu ciclo de vida.

Por que esse controle é crítico?

Os dados ultrapassam os limites da organização, estando na nuvem, nas casas dos agentes públicos, em dispositivos portáteis e compartilhados com parceiros, o que demanda gestão e proteções adequadas ao longo de todo o ciclo de vida dos dados, incluindo aspectos de conformidade.

Além dos dados críticos para as estratégias dos diferentes órgãos, existem dados relacionados a finanças, propriedade intelectual e dados de cidadãos custodiados pela organização. Invasores buscam extrair esses dados confidenciais, mas muitas organizações não monitoram o tráfego de saída, ficando vulneráveis. Além de ataques na rede, há riscos como roubo físico de dispositivos e ameaças à parceiros que armazenam esses dados. A perda de controle sobre esses dados gera impactos graves, muitas vezes decorrentes de má gestão e erros humanos.

Procedimentos e ferramentas

É fundamental que a organização estabeleça um processo de gerenciamento de dados com diretrizes para categorização, proteção, manuseio, retenção e descarte. Também deve haver um processo para tratar possíveis violações de dados que se integre ao plano de resposta a incidentes e aos planos de conformidade e comunicação. Os dados devem ser categorizados considerando os diferentes níveis de criticidade. Em seguida, criar um inventário que mapeie os dados, os softwares que os acessam e os ativos que os hospedam. A rede deve ser segmentada conforme níveis de criticidade, considerando a utilização de *firewalls* ou outros recursos tecnológicos para controlar o acesso a cada segmento e aplicando regras de acesso de usuários para permitir o acesso aos dados apenas àqueles que realmente necessitam.

Para uma abordagem mais abrangente deste tópico, os seguintes recursos podem ser consultados para auxiliar na proteção de dados:

- NIST® SP 800-88r2 Diretrizes para sanitização de mídias: https://csrc.nist.gov/pubs/sp/800/88/r2/final

- NIST® FIPS 140-3 Requisitos de Segurança para Módulos Criptográficos: https://csrc.nist.gov/pubs/fips/140-3/final
- Guia Complementar de Segurança da Informação para Computação em Nuvem: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi-2.0/
- Guia Complementar do CIS *Controls* para Dispositivos Móveis: https://www.cisecurity.org/controls/resources?crc=environment-specific-guidance

Lista de medidas

ID	Título, descrição e normas de referência	GI
3.1	**O órgão estabelece e mantém um processo de gestão de dados?**	GI1
	Estabelecer e manter um processo de gestão de dados. No processo, tratar a criticidade, o proprietário, o manuseio, os limites de retenção e os requisitos para descarte dos dados com base em padrões de criticidade e retenção da organização. Revisar e atualizar a documentação anualmente ou quando ocorrerem mudanças significativas na organização que possam impactar esta medida.	
	Normas de referência: IN GSI/PR nº 3/2021, Capítulo II; *IN GSI/PR nº 5/2021, Capítulo IV, Seção VII; NC nº 20/IN01/DSIC/GSIPR, item 7; **IN GSI/PR nº 8/2025, arts. 4º, 5º e 6º.	
3.2	**O órgão estabelece e mantém um inventário de dados?**	GI1
	Estabelecer e manter um inventário de dados - priorizando os dados críticos, sigilosos e com restrição de acesso - com base no processo de gestão de dados. Realizar a revisão e atualização periódica do inventário. O inventário de dados pessoais é objeto do Controle 19.	
	Normas de referência: IN GSI/PR nº 3/2021, Capítulo II.	
3.3	**O órgão configura listas de controle de acesso a dados?**	GI1
	Configurar listas de controle de acesso a dados com base no princípio da necessidade de saber do usuário. Aplicar listas de controle de acesso, também conhecidas como permissões de acesso, a sistemas de arquivos locais e remotos, bancos de dados e aplicações.	
	Normas de referência: **IN GSI/PR nº 8/2025, art. 3º, VIII e XIII.	
3.4	**O órgão aplica retenção de dados?**	GI1
	Reter os dados de acordo com o processo de gestão de dados e a legislação vigente. A retenção deve incluir prazos mínimos e máximos.	
	Normas de referência: NC nº 20/IN01/DSIC/GSIPR, itens 6.2 e 6.4.	
3.5	**O órgão descarta dados com segurança?**	GI1
	Descartar com segurança os dados, sejam eles armazenados em meio físico ou lógico, conforme o processo de gestão de dados e a legislação vigente. Certificar-se de que o método de descarte adotado seja compatível com a criticidade dos dados.	

Normas de referência: NC nº 20/IN01/DSIC/GSIPR, item 6.4.

3.6	O órgão criptografa dados críticos em dispositivos de usuário final?	GI1

Criptografar os dados críticos para a organização em dispositivos de usuário final, considerando a NC nº 09/IN01/DSIC/GSIPR.

Normas de referência: IN GSI/PR nº 3/2013; NC nº 09/IN01/DSIC/GSIPR.

3.7	O órgão estabelece e mantém um esquema de classificação de dados?	GI2

Estabelecer e manter um esquema geral de classificação de dados baseado na criticidade para a organização, com critérios para classificação específicos. Revisar e atualizar o esquema de classificação anualmente ou quando ocorrerem mudanças significativas que possam impactar esta medida.

Normas de referência: IN GSI/PR nº 3/2021, Capítulo II.

3.8	O órgão documenta os fluxos de dados?	GI2

Documentar o fluxo de dados com base no processo de gestão de dados, garantindo rastreabilidade e conformidade com normas e diretrizes. A documentação do fluxo de dados deve ser revisada e atualizada anualmente ou sempre que houver mudanças significativas que possam impactá-lo.

Normas de referência: IN GSI/PR nº 3/2021, Capítulo II.

3.9	O órgão criptografa dados críticos em mídia removível?	GI2

Criptografar os dados críticos para a organização em mídias removíveis, considerando a NC nº 09/IN01/DSIC/GSIPR.

Normas de referência: IN GSI/PR nº 3/2013; NC nº 09/IN01/DSIC/GSIPR.

3.10	O órgão criptografa os dados críticos que estão em trânsito?	GI2

Criptografar os dados críticos para a organização que estão em trânsito, considerando a NC nº 09/IN01/DSIC/GSIPR.

Normas de referência: NC nº 09/IN01/DSIC/GSIPR; IN GSI/PR nº 5/2021, Capítulo IV, Seção IV; *IN GSI/PR nº 5/2021, Capítulo IV, Seção IV; **IN GSI/PR nº 8/2025, art. 3º, IV e V

3.11	O órgão criptografa os dados críticos que estão em repouso?	GI2

Criptografar os dados críticos para a organização e que estão em repouso nos servidores, sistemas e banco de dados que os armazenam, considerando a NC nº 09/IN01/DSIC/GSIPR.

Normas de referência: NC nº 09/IN01/DSIC/GSIPR; IN GSI/PR nº 5/2021, Capítulo IV, Seção IV; *IN GSI/PR nº 5/2021, Capítulo IV, Seção IV; **IN GSI/PR nº 8/2025, art. 3º, IV e V.

3.12	O órgão segmenta o processamento e o armazenamento de dados com base na criticidade?	GI2
Segmentar o processamento e armazenamento de dados com base na sua criticidade. Não processar dados críticos para a organização em ativos institucionais destinados a dados de menor criticidade.		
Normas de referência: *IN GSI/PR nº 5/2021, Capítulo IV, Seção V; **IN GSI/PR nº 8/2025, art. 3º, I, II, III.		

3.13	O órgão implanta uma solução de prevenção contra perda de dados?	GI3
Implementar uma ferramenta automatizada, como uma solução de prevenção de perda de dados (*Data Loss Prevention*, DLP) baseada em host, para identificar todos os dados críticos processados, transmitidos ou armazenados por meio dos ativos institucionais.		
Normas de referência: não identificada.		

3.14	O órgão registra o acesso aos dados críticos?	GI3
Registrar o acesso aos dados críticos para a organização, incluindo modificação e descarte.		
Normas de referência: NC nº 21/IN01/DSIC/GSIPR, 6.2, b; *IN GSI/PR nº 5/2021, Capítulo IV, Seção III; **IN GSI/PR nº 8/2025, art. 3º, IX.		

* A IN GSI/PR nº 5/2021 estabelece os requisitos mínimos de segurança da informação para que órgãos e entidades da administração pública federal utilizem soluções de computação em nuvem, sendo uma norma de referência apenas para estes ambientes computacionais.

** A IN GSI/PR nº 8/2025 estabelece os requisitos mínimos de segurança da informação para tratamento de informação classificada em computação em nuvem, sendo uma norma de referência apenas para estas situações.

5.4 CONTROLE 4: Configuração segura de ativos institucionais e soluções de *software*

Visão geral

Estabelecer e manter a configuração segura de dispositivos de usuário final, incluindo portáteis e móveis, dispositivos de rede, dispositivos não computacionais/IoT e servidores, além de soluções de *software*.

Por que esse controle é crítico?

Configurações padrão de ativos institucionais são focadas em facilidade de uso, não segurança, deixando vulnerabilidades como portas abertas, contas padrão, e soluções de *software* desnecessários instalados que podem ser explorados por atacantes. Configurações seguras devem ser mantidas e gerenciadas durante todo o ciclo de vida dos ativos para evitar degradação da segurança devido a atualizações, mudanças ou instalações de novas soluções de *software*. Isso se aplica a todos os ativos institucionais e ambientes computacionais, incluindo dispositivos locais, remotos, de rede e computação em nuvem.

Procedimentos e ferramentas

Recomenda-se a utilização de *benchmarks* públicos, guias, e *checklists* de segurança como CIS *Benchmarks* e NIST para estabelecer configurações seguras de ativos institucionais. Configurações padrão podem ser automatizadas com scripts de segurança e ferramentas para medir a conformidade. Ferramentas comerciais podem aplicar configurações seguras automaticamente por agentes de *software* ou remotamente.

Alguns recursos para apoiar a implementação deste controle incluem:

- Ferramenta de Avaliação de Configuração do CIS (CIS *Configuration Assessment Tool*, CIS-CAT®): https://learn.cisecurity.org/cis-cat-lite
- CIS *Benchmarks® Program*: http://www.cisecurity.org/cis-benchmarks/
- NIST® *National Checklist Program* (NCP): https://nvd.nist.gov/ncp/repository

Lista de medidas

ID	Título, descrição e normas de referência	GI
4.1	**O órgão estabelece e mantém um processo de configuração segura?**	GI1
	Estabelecer e manter um processo de configuração segura para os ativos institucionais (dispositivos de usuário final, incluindo portáteis e móveis, dispositivos da IOT e não computacionais, servidores) e soluções de software. Revisar e atualizar a documentação anualmente ou quando ocorrerem mudanças significativas na organização que possam impactar esta medida.	
	Normas de referência: não identificada.	
4.2	**O órgão estabelece e mantém um processo de configuração segura para a infraestrutura de rede?**	GI1
	Estabelecer e manter um processo de configuração segura para dispositivos de rede. Revisar e atualizar a documentação anualmente ou quando ocorrerem mudanças significativas na organização que possam impactar esta medida.	
	Normas de referência: não identificada.	
4.3	**O órgão configura o bloqueio automático de sessão nos ativos institucionais?**	GI1
	Configurar o bloqueio automático de sessão, quando aplicável, nos ativos institucionais após um período definido de inatividade.	
	Normas de referência: não identificada.	
4.4	**O órgão implementa e gerencia um *firewall* nos servidores?**	GI1
	Implementar e gerenciar um *firewall* nos servidores, quando suportado.	
	Normas de referência: não identificada.	

4.5	**O órgão implementa e gerencia um *firewall* em dispositivos do usuário final?**	**GI1**

Implementar e gerenciar um *firewall* baseado em host ou uma ferramenta de filtragem de porta nos dispositivos de usuário final, com uma regra de negação padrão que bloqueia todo o tráfego, exceto os serviços e portas que são explicitamente permitidos.

Normas de referência: não identificada.

4.6	**O órgão gerencia com segurança os ativos institucionais e soluções de software?**	**GI1**

Gerenciar com segurança os ativos institucionais e soluções de software. Exemplos de implementações incluem gestão de configuração por meio de infraestrutura como código com controle de versão (*version controlled-infrastructure-as-code*) e acesso a interfaces administrativas por meio de protocolos de rede seguros.

Normas de referência: não identificada.

4.7	**O órgão gerencia contas padrão?**	**GI1**

Gerenciar contas padrão nos ativos institucionais e soluções de software, como root, administrador e outras contas de fornecedores pré-configuradas.

Normas de referência: não identificada.

4.8	**O órgão desinstala ou desativa serviços desnecessários?**	**GI2**

Desinstalar ou desativar serviços desnecessários nos ativos institucionais e soluções de software, como serviço de compartilhamento de arquivo não utilizado, módulo de aplicação web ou função de serviço.

Normas de referência: não identificada.

4.9	**O órgão configura servidores Sistema de Nomes de Domínio (*Domain Name System*, DNS) confiáveis?**	**GI2**

Configurar servidores DNS confiáveis nos ativos institucionais. Exemplos de implementações incluem configurar a infraestrutura de rede para usar servidores DNS controlados pela organização ou servidores DNS externos confiáveis.

Normas de referência: não identificada.

4.10	**O órgão aplica o recurso de bloqueio automático nos dispositivos portáteis de usuário final?**	**GI2**

Aplicar o bloqueio automático dos dispositivos portáteis de usuário final após um número de tentativas de autenticação com falha, com base no limite definido pela organização.

Normas de referência: não identificada.

4.11	O órgão aplica o recurso de limpeza remota nos dispositivos portáteis de usuário final?	GI2
Assegurar que os dispositivos portáteis de usuário final de propriedade da organização estejam preparados para limpeza remota e executá-la conforme previsto na política de gestão de ativos institucionais, incluindo casos como dispositivos perdidos ou roubados, ou quando um indivíduo não trabalha mais na organização.		
Normas de referência: não identificada.		

4.12	O órgão separa os espaços de trabalho nos dispositivos móveis?	GI3
Certificar de que a separação de espaços de trabalho seja usada nos dispositivos móveis de usuário final, ou seja, separar aplicações e dados institucionais de aplicações e dados de uso pessoal nos dispositivos, quando suportado.		
Normas de referência: não identificada.		

5.5 CONTROLE 5: Gestão de contas

Visão geral

Aplicar processos e ferramentas para atribuir e gerenciar autorização para credenciais de contas de usuário e contas de serviços.

Por que esse controle é crítico?

Acesso não autorizado por credenciais válidas é uma das formas mais fáceis de invasão. Existem muitas maneiras de obter acesso às contas de usuários secretamente, incluindo: senhas fracas, contas ainda válidas após um agente público sair do órgão, contas de teste inativas ou persistentes, contas compartilhadas que não foram alteradas em meses ou anos, contas de serviço incorporadas em aplicativos para *scripts*, um usuário com a mesma senha que a usa para uma conta *online* que foi comprometida (em um *dump* público de senhas), engenharia social para que um usuário forneça sua senha ou uso de *malware* para capturar senhas ou *tokens* na memória ou na rede.

Contas administrativas são alvos prioritários por permitirem a adição de outras contas, além de alteração nos ativos para torná-los mais vulneráveis, além de possuírem outros privilégios que podem impactar mais ainda o órgão. Contas de serviço também são importantes, pois geralmente são compartilhadas entre equipes, internas e externas ao órgão, e às vezes não são conhecidas, muitas vezes são reveladas em auditorias.

Sendo assim, o monitoramento e auditoria de contas são essenciais para reduzir riscos causados por comportamento interno ou externo.

Procedimentos e ferramentas

Contas devem ser inventariadas, auditadas periodicamente e controladas, especialmente para contas administrativas ou de alto privilégio e contas de serviço. Contas inativas devem ser desabilitadas e, caso apropriado, removida do ativo. Recomenda-se que usuários com acesso de administrador ou outro privilégio tenham contas separadas para essas tarefas de autoridade superior.

A adoção de *Single Sign-On* (SSO) é recomendada quando uma organização possui muitas soluções de *software*, ajudando a reduzir o número de senhas que um usuário precisa gerenciar. Sugere-se também que os ativos sejam configurados para desconectar os usuários automaticamente após um período de inatividade.

Recomenda-se que os usuários utilizem gerenciadores de senhas para armazenar suas senhas com segurança e sejam orientados para bloquear a tela ao se ausentar do dispositivo.

Alguns recursos relevantes para apoio na implementação deste controle são:

- Diretrizes de Identidade Digital do NIST®: https://pages.nist.gov/800-63-3/
- Guia de Política de Senhas do CIS: https://www.cisecurity.org/white-papers/cis-password-policy-guide

Lista de medidas

ID	Título, descrição e normas de referência	GI
5.1	**O órgão estabelece e mantém um inventário de contas?**	**GI1**
Estabelecer e manter um inventário de todas as contas gerenciadas na organização. O inventário deve incluir contas de usuário e de administrador, e conter minimamente o nome do agente público, o nome do usuário, datas de início e término, além do departamento. Validar se todas as contas ativas estão autorizadas, trimestralmente ou em intervalos menores.		
Normas de referência: IN GSI/PR nº 3/2021, Capítulo II.		
5.2	**O órgão promove ações para evitar a reutilização de senhas?**	**GI1**
Configurar os ativos institucionais para evitar ou desestimular a reutilização de senhas, promovendo a adoção de senhas únicas para ativos diferentes.		
Normas de referência: não identificada.		
5.3	**O órgão desabilita ou exclui contas inativas?**	**GI1**
Desabilitar ou excluir quaisquer contas inativas, conforme política de gestão de contas, após um período de inatividade estabelecido pela organização.		
Normas de referência: não identificada.		
5.4	**O órgão limita os privilégios de administrador às contas de administrador dedicadas?**	**GI1**

Limitar os privilégios de administrador às contas de administrador dedicadas. Realizar atividades gerais de computação, como navegação na Internet, e-mail e uso do pacote de produtividade, a partir da conta primária não privilegiada do usuário.	
Normas de referência: não identificada.	
5.5 O órgão estabelece e mantém um inventário de contas de serviço?	**GI2**
Estabelecer e manter um inventário de contas de serviço. O inventário, no mínimo, deve conter a unidade proprietária, data de revisão e propósito. Realizar revisões de contas de serviço para validar se todas as contas ativas estão autorizadas, em uma programação recorrente, no mínimo trimestralmente ou em intervalos menores.	
Normas de referência: IN GSI/PR nº 3/2021, Capítulo II.	
5.6 O órgão centraliza a gestão de contas?	**GI2**
Centralizar a gestão de contas por meio de serviço de diretório ou de identidade.	
Normas de referência: *IN GSI/PR nº 5/2021, art. 13, I, II e II; **IN GSI/PR nº 8/2025, art. 3º, XI.	

* A IN GSI/PR nº 5/2021 estabelece os requisitos mínimos de segurança da informação para que órgãos e entidades da administração pública federal utilizem soluções de computação em nuvem, sendo uma norma de referência apenas para estes ambientes computacionais.
** A IN GSI/PR nº 8/2025 estabelece os requisitos mínimos de segurança da informação para tratamento de informação classificada em computação em nuvem, sendo uma norma de referência apenas para estas situações.

5.6 CONTROLE 6: Gestão de acesso

Visão geral

Aplicar processos e ferramentas para criar, atribuir, gerenciar e revogar credenciais de acesso e privilégios para contas de usuário, administrador e serviço para ativos de informação.

Por que esse controle é crítico?

Enquanto o controle 5 trata especificamente do gerenciamento de contas, este controle concentra-se em gerenciar o acesso dessas contas, garantindo que os usuários tenham acesso apenas aos ativos de informação necessários para sua função, garantindo que haja autenticação forte para acesso à dados ou funções organizacionais críticas.

Controlar o acesso aos ativos é crucial para limitar o impacto de comprometimentos dos ativos. Privilégios mal distribuídos facilitam ataques internos e externos, especialmente para contas administrativas. MFA e ferramentas de gerenciamento de acesso privilegiado fortalecem a segurança.

Procedimentos e ferramentas

Processos documentados devem ser usados para concessão e revogação de privilégios, preferencialmente automatizados. Idealmente, o controle de acesso baseado em funções deve ser adotado e revisado regularmente. MFA é vital para acessos externos e privilegiados. Ferramentas para centralizar e gerenciar autenticação, autorização e MFA são essenciais.

O desprovisionamento abrangente de contas é importante e deve incluir todas as contas de usuário, desde servidores até terceirizados. As organizações também devem inventariar e rastrear contas de serviço, pois um erro comum é deixar *tokens* ou senhas em texto não criptografado no código e publicá-los em repositórios de código baseados em nuvem pública.

A equipe de segurança deve monitorar e identificar periodicamente processos em execução para determinar se algum navegador, leitor de *e-mail* e demais soluções de *software* estão sendo executados com privilégios altos.

- Um recurso relevante é a publicação Diretrizes de Identidade Digital do NIST®: https://pages.nist.gov/800-63-3/

Lista de medidas

ID	Título, descrição e normas de referência	GI
6.1	**O órgão estabelece um processo de concessão de acesso?**	**GI1**
Estabelecer e manter um processo, de preferência automatizado, para conceder acesso físico e lógico aos ativos institucionais e soluções de software mediante novo ingresso de agente público, concessão de direitos ou mudança de função de um usuário.		
Normas de referência: não identificada.		
6.2	**O órgão estabelece um processo de revogação de acesso?**	**GI1**
Estabelecer e manter um processo, de preferência automatizado, para revogar o acesso aos ativos institucionais e soluções de software, por meio da desativação de contas imediatamente após seu encerramento, revogação de direitos ou mudança de função de um usuário. Desativar contas, em vez de excluí-las, pode ser necessário para preservar as trilhas de auditoria.		
Normas de referência: não identificada.		
6.3	**O órgão exige autenticação multifator (*Multi-Factor Authentication*, MFA) para soluções de software expostas externamente?**	**GI1**
Exigir que todas as soluções de software da organização ou de terceiros expostas externamente apliquem autenticação multifator, onde suportado. Aplicar autenticação multifator por meio de um serviço de diretório ou provedor de *Single Sign-On* (SSO) é uma forma de implementação desta medida.		
Normas de referência: *IN GSI/PR nº 5/2021, art. 13, I, II e III; **IN GSI/PR nº 8/2025, art. 3º, VII.		

6.4	**O órgão exige autenticação multifator (*Multi-Factor Authentication*, MFA) para acesso remoto à rede?**	**GI1**

Exigir autenticação multifator para acesso remoto à rede.

Normas de referência: não identificada.

6.5	**O órgão exige autenticação multifator (*Multi-Factor Authentication*, MFA) para acesso administrativo?**	**GI1**

Exigir autenticação multifator para todas as contas de acesso administrativo, em todos os ativos institucionais e soluções de software, sejam gerenciados no site local ou por meio de um provedor terceirizado.

Normas de referência: não identificada.

6.6	**O órgão estabelece e mantém um inventário de sistemas de autenticação e autorização?**	**GI2**

Estabelecer e manter um inventário dos sistemas de autenticação e autorização da organização, incluindo aqueles hospedados no site local ou em um provedor de serviços remoto. Revisar e atualizar o inventário semestralmente ou em intervalos menores.

Normas de referência: IN GSI/PR nº 3/2021, Capítulo II.

6.7	**O órgão centraliza o controle de acesso?**	**GI2**

Centralizar o controle de acesso para todos os ativos institucionais e soluções de software por meio de um serviço de diretório ou provedor de *Single Sign-On* (SSO), quando suportado.

Normas de referência: *IN GSI/PR nº 5/2021, art. 13, III; **IN GSI/PR nº 8/2025, art. 3º, XI.

6.8	**O órgão define e mantém o controle de acesso baseado em funções?**	**GI3**

Definir e manter o controle de acesso baseado em funções, determinando e documentando os direitos de acesso necessários para cada função dentro da organização para cumprir com sucesso as funções atribuídas. Revisar os controles de acesso para validar se todos os privilégios estão autorizados, em uma programação recorrente, uma vez por ano ou em intervalos menores.

Normas de referência: **IN GSI/PR nº 8/2025, art. 3º, XII.

* A IN GSI/PR nº 5/2021 estabelece os requisitos mínimos de segurança da informação para que órgãos e entidades da administração pública federal utilizem soluções de computação em nuvem, sendo uma norma de referência apenas para estes ambientes computacionais.

** A IN GSI/PR nº 8/2025 estabelece os requisitos mínimos de segurança da informação para tratamento de informação classificada em computação em nuvem, sendo uma norma de referência apenas para estas situações.

5.7 CONTROLE 7: Gestão contínua de vulnerabilidades

Visão geral

Desenvolver um plano para avaliar e monitorar continuamente vulnerabilidades em todos os ativos de informação da organização, a fim de remediar e minimizar a janela de oportunidade para atacantes. Monitorar fontes públicas e privadas em busca de novas informações sobre ameaças e vulnerabilidades.

Por que esse controle é crítico?

Vulnerabilidades são alvo constante de atacantes. As equipes de segurança devem acompanhar de forma ágil informações sobre: atualizações de soluções *software*, *patches*, alertas de segurança, boletins de ameaças, entre outros, e devem revisar regularmente seu ambiente para identificar vulnerabilidades antes que os invasores o façam. Vulnerabilidades novas ou desconhecidas ("*zero-day*") aumentam o risco e as equipes precisam estar ciente desta possibilidade pois podem precisar implementar outros controles para mitigar o risco.

As organizações que não avaliam sua infraestrutura em busca de vulnerabilidades e não abordam proativamente as falhas descobertas enfrentam uma probabilidade significativa de ter seus ativos de informação comprometidos. Sem gestão contínua, o ambiente fica vulnerável a explorações.

Procedimentos e ferramentas

Planos documentados para gestão de vulnerabilidades são necessários. Ferramentas de varredura automatizada, tanto autenticada quanto não autenticada, devem ser usadas regularmente para identificar vulnerabilidades internas e externas. Para ajudar a padronizar as definições de vulnerabilidades descobertas em uma organização, é preferível usar ferramentas de varredura de vulnerabilidades que mapeiem vulnerabilidades para um ou mais dos seguintes esquemas e linguagens de classificação de vulnerabilidades, configurações e plataformas especificadas na publicação NIST SP 800-126r3[2]: *Common Vulnerabilities and Exposures* (CVE®), *Common Configuration Enumeration* (CCE), *Open Vulnerability and Assessment Language* (OVAL®), *Common Platform Enumeration* (CPE), *Common Vulnerability Scoring System* (CVSS) ou *Extensible Configuration Checklist Description Format* (XCCDF). A remediação deve ser priorizada e executada conforme os riscos.

Além das varreduras, outras ferramentas analisam configurações de segurança e identificam mudanças não autorizadas ou vulnerabilidades introduzidas inadvertidamente. Organizações eficientes conectam *scanners* a sistemas de emissão de *tickets* para acompanhar a correção de vulnerabilidades e reportar à alta gerência, permitindo priorização e cumprimento de requisitos de conformidade.

[2] Disponível em https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-126r3.pdf

Deve haver um processo de garantia de qualidade para verificar se as atualizações de configuração ou se os patches foram implementados corretamente em todos os ativos institucionais relevantes.

Por fim, recomenda-se o seguinte recurso dedicado a este tema:

- serviço de análise de vulnerabilidades do Centro Integrado de Segurança Cibernética (CISC GOV.BR): https://www.gov.br/cisc/pt-br

Lista de medidas

ID	Título, descrição e normas de referência	GI
7.1	**O órgão estabelece e mantém um processo de gestão de vulnerabilidade?**	GI1
	Estabelecer e manter um processo de gestão de vulnerabilidade para ativos institucionais e soluções de software. Revisar e atualizar a documentação anualmente ou quando ocorrerem mudanças significativas na organização que possam impactar esta medida.	
	Normas de referência: IN GSI/PR nº 3/2021, Capítulo III.	
7.2	**O órgão estabelece e mantém um processo de remediação?**	GI1
	Estabelecer e manter um processo de remediação, fundamentado na estratégia de remediação institucional baseada em risco, com revisões semestrais ou em intervalos menores.	
	Normas de referência: IN GSI/PR nº 3/2021, Capítulo III.	
7.3	**O órgão executa a gestão automatizada de atualizações do sistema operacional?**	GI1
	Realizar atualizações do sistema operacional por meio da gestão automatizada de atualizações, mensalmente ou com mais frequência.	
	Normas de referência: não identificada.	
7.4	**O órgão executa a gestão automatizada de atualizações de aplicações?**	GI1
	Realizar atualizações de aplicações por meio da gestão automatizada de atualizações, mensalmente ou em intervalos menores.	
	Normas de referência: não identificada.	
7.5	**O órgão realiza varreduras automatizadas de vulnerabilidades internas?**	GI2
	Realizar varreduras automatizadas de vulnerabilidade em ativos institucionais e soluções de software internos, trimestralmente ou em intervalos menores. Realizar varreduras autenticadas e não autenticadas.	
	Normas de referência: não identificada.	

7.6	O órgão realiza varreduras automatizadas de vulnerabilidades expostas externamente?	GI2
Executar varreduras de vulnerabilidade automatizadas nos ativos institucionais e soluções de software expostos externamente. Executar varreduras mensalmente ou em intervalos menores.		
Normas de referência: não identificada.		
7.7	O órgão corrige vulnerabilidades detectadas?	GI2
Corrigir as vulnerabilidades detectadas por meio de processos e ferramentas, mensalmente ou em intervalos menores, com base no processo de remediação.		
Normas de referência: IN GSI/PR nº 3/2021, Capítulo III.		

5.8 CONTROLE 8: Gestão de registros de auditoria

Visão geral

Coletar, alertar, analisar e reter registros de auditoria de eventos que possam ajudar a detectar, compreender ou se recuperar de um ataque.

Por que esse controle é crítico?

Coletar e analisar *logs* são atividades essenciais para detectar atividades maliciosas. Muitos ataques só são descobertos por análise de *logs*, algumas vezes sendo a única evidência de um ataque bem-sucedido. Os registros de *log* também são cruciais para a resposta a incidentes. Após a detecção de um ataque, a análise de *logs* pode ajudar as organizações a compreenderem a extensão do ataque - quando e como o ataque ocorreu, quais informações foram acessadas e se os dados foram exfiltrados.

No entanto, muitas organizações não monitoram ou analisam esses registros adequadamente, permitindo invasores agirem por muito tempo sem serem detectados. *Logs* também são fundamentais para investigações e conformidade regulatória.

Procedimentos e ferramentas

A maioria dos ativos institucionais e soluções de *software* oferecem recurso para registro de *logs*, o qual recomenda-se que seja ativado e configurado para envio para servidores de *logs* centralizados. *Firewalls*, *proxies* e sistemas de acesso remoto devem ser configurados para registro detalhado, quando necessário. A retenção dos *logs* também é importante caso seja necessária uma investigação de incidente, e o prazo deve estar de acordo com a legislação vigente aplicável.

Além disso, todos os ativos institucionais e soluções de *software* devem ser configurados para criar registros de controle de acesso quando um usuário tenta acessar recursos sem os

privilégios apropriados. Para avaliar se esse registro está em vigor, uma organização deve verificar periodicamente seus registros e compará-los com o inventário de ativos institucionais e soluções de *software* reunidos como parte dos controles 1 e 2, a fim de garantir que cada item dos inventários esteja gerando registros periodicamente.

Lista de medidas

ID	Título, descrição e normas de referência	GI
8.1	**O órgão estabelece e mantém um processo de gestão de *logs* de auditoria?**	GI1
	Estabelecer e manter um processo de gestão de *logs* de auditoria que defina os requisitos de registro de *logs* da organização, considerando a NC nº 21/IN01/DSIC/GSIPR. No mínimo, abordar a coleta, revisão e armazenamento dos *logs* de auditoria para os ativos institucionais e soluções de software, considerando o tempo de retenção e os dados estritamente necessários à segurança da informação. Revisar e atualizar a documentação anualmente ou sempre que ocorrerem mudanças significativas na organização que possam impactar esta medida.	
	Normas de referência: NC nº 21/IN01/DSIC/GSIPR; *IN GSI/PR nº 5/2021, art. 13, IV, V e VI.	
8.2	**O órgão coleta *logs* de auditoria?**	GI1
	Coletar *logs* de auditoria. Certificar-se de que o *log*, de acordo com o processo de gestão de *log* de auditoria da organização, tenha sido habilitado em todos os ativos institucionais e soluções de software em que esta funcionalidade estiver disponível.	
	Normas de referência: NC nº 21/IN01/DSIC/GSIPR, 6.2; *IN GSI/PR nº 5/2021, art. 13, IV, V e VI.	
8.3	**O órgão armazena adequadamente os *logs* de auditoria?**	GI1
	Assegurar que os *logs* possuam armazenamento seguro em conformidade com normas internas e regulatórias, preservando sua integridade e proteção contra alterações. Além disso, garantir acessibilidade e monitoramento contínuo, assegurando a disponibilidade dos *logs* para auditorias e investigações, bem como a aderência aos normativos aplicáveis, em atendimento aos requisitos de gerenciamento de registros de auditoria da organização.	
	Normas de referência: *IN GSI/PR nº 5/2021, art. 13, IV, V e VI.	
8.4	**O órgão padroniza a sincronização de tempo?**	GI2
	Padronizar a sincronização de tempo. Configurar todos os ativos institucionais e soluções de software com pelo menos duas fontes de sincronização de tempo, quando suportado.	
	Normas de referência: NC nº 21/IN01/DSIC/GSIPR, 6.1.	
8.5	**O órgão coleta *logs* de auditoria detalhados?**	GI2

Configurar o *log* de auditoria detalhado para os ativos institucionais e soluções de software que contenham dados críticos para a organização. Incluir a origem do evento, data, nome de usuário, carimbo de data e hora, endereços de origem, endereços de destino e outros elementos úteis que possam ajudar em uma investigação forense.

Normas de referência: NC nº 21/IN01/DSIC/GSIPR, 6.3.

8.6	**O órgão coleta *logs* de auditoria de consulta do Sistema de Nomes de Domínio (*Domain Name System*, DNS)?**	**GI2**

Habilitar o registro de *log* de consulta do servidor DNS inclusive para detectar pesquisas de nomes de *host* para domínios maliciosos conhecidos, quando suportado.

Normas de referência: não identificada.

8.7	**O órgão coleta *logs* de auditoria de requisição de *Uniform Resource Locator* (URL)?**	**GI2**

Coletar *logs* de auditoria de requisição de URL em ativos institucionais, quando suportado.

Normas de referência: não identificada.

8.8	**O órgão coleta *logs* de auditoria de linha de comando?**	**GI2**

Habilitar o *log* de auditoria sobre ferramentas de linha de comando, tais como Microsoft Powershell, Bash e demais terminais administrativos remotos.

Normas de referência: não identificada.

8.9	**O órgão centraliza os *logs* de auditoria?**	**GI2**

Centralizar, sempre que possível, a coleta e retenção de *logs* de auditoria de acordo com um processo de gerenciamento de *logs* de auditoria.

Normas de referência: NC nº 21/IN01/DSIC/GSIPR, 6.8.

8.10	**O órgão retém os *logs* de auditoria?**	**GI2**

Garantir a retenção dos *logs* de auditoria pelo período estabelecido pela organização.

Normas de referência: NC nº 21/IN01/DSIC/GSIPR, 6.7; *IN GSI/PR nº 5/2021, art. 13, IV, V e VI.

8.11	**O órgão conduz revisões de *logs* de auditoria?**	**GI2**

Realizar análises de *logs* de auditoria para detectar anomalias ou eventos anormais que possam indicar uma ameaça potencial. Realizar revisões semanalmente ou em intervalos menores.

Normas de referência: não identificada.

8.12	**O órgão coleta *logs* de provedores de serviços?**	**GI3**

Coletar *logs* de provedores de serviços, quando suportado. Exemplos de implementações incluem coleta de eventos de autenticação e autorização, eventos de criação e de descarte de dados e eventos de gestão de usuários.
Normas de referência: *IN GSI/PR nº 5/2021, art. 13, IV, V e VI

* A IN GSI/PR nº 5/2021 estabelece os requisitos mínimos de segurança da informação para que órgãos e entidades da administração pública federal utilizem soluções de computação em nuvem, sendo uma norma de referência apenas para estes ambientes computacionais.

5.9 CONTROLE 9: Proteção de *e-mail* e navegador *web*

Visão geral

Aprimorar as proteções e detecções de ameaças provenientes de *e-mails* e da *web*, pois essas são oportunidades para invasores manipularem o comportamento humano por meio de diferentes técnicas.

Por que esse controle é crítico?

E-mail e navegadores *web* são vetores comuns para diferentes tipos de ataques, incluindo engenharia social e *malware*, pois estão diretamente expostos aos usuários. *Malwares* exploram vulnerabilidades de navegadores e suas extensões. Por sua vez, os *e-mails* são os principais canais para *phishing*, impactando a segurança das organizações.

Procedimentos e ferramentas

Manter apenas versões suportadas pelos seus fabricantes de navegadores (incluindo suas extensões) e clientes de *e-mail*. Restringir extensões não autorizadas e de fontes não confiáveis. Usar filtros DNS nativos dos navegadores para bloquear sites maliciosos, além de filtros de URL na rede. Considerar também a assinatura de serviços de filtragem de DNS para bloquear tentativas de acesso.

Implementar filtragem de *spam* e verificação de *malware* no *gateway* de *e-mail*, bem como *Domain-Based Message Authentication, Reporting, and Conformance* (DMARC), ajuda a reduzir atividades de *spam* e *phishing*. Além de filtros com base no remetente, recomenda-se bloquear tipos de arquivos não necessários no *gateway* de *e-mail*. A instalação de uma ferramenta de criptografia para proteger *e-mails* e comunicações adiciona outra camada de segurança para o usuário e para a rede. Proteções de antivírus e *sandboxing* para servidores de *e-mail* também são fatores que auxiliam na mitigação do risco.

Como os ataques de *phishing* por *e-mail* evoluem constantemente para burlar os filtros de *spam*, antivírus, *sandboxing* e demais medidas técnicas de segurança da informação, é fundamental conscientizar os agentes públicos para que saibam identificar mensagens suspeitas e as reportem à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR). Realizar simulações regulares de *phishing* é uma prática eficaz para

conscientizar os agentes públicos, ajudando-os a reconhecer diferentes tipos de ataques e a acompanhar a evolução dessas ameaças ao longo do tempo.

Lista de medidas

ID	Título, descrição e normas de referência	GI
9.1	**O órgão permite o uso apenas de navegadores e clientes de e-mail totalmente suportados por seus fornecedores?**	GI1
	Assegurar que apenas navegadores e clientes de e-mail totalmente suportados por seus fornecedores tenham permissão para executar na organização, usando apenas a versão mais recente.	
	Normas de referência: não identificada.	
9.2	**O órgão usa serviços de filtragem de Sistema de Nomes de Domínio (*Domain Name System*, DNS?**	GI1
	Usar serviços de filtragem de DNS em todos os dispositivos do usuário final, incluindo ativos remotos e locais, para bloquear o acesso a domínios maliciosos conhecidos.	
	Normas de referência: não identificada.	
9.3	**O órgão mantém e aplica filtros de *Uniform Resource Locator* (URL) baseados em rede?**	GI2
	Aplicar e atualizar filtros de URL baseados em rede para limitar os ativos institucionais de se conectarem a sites potencialmente maliciosos ou não aprovados.	
	Normas de referência: não identificada.	
9.4	**O órgão restringe extensões desnecessárias ou não autorizadas de navegadores e clientes de e-mail?**	GI2
	Restringir, por meio de desinstalação ou desativação, quaisquer *plug-ins*, extensões e aplicativos complementares não autorizados ou desnecessários de navegadores ou de clientes de e-mail.	
	Normas de referência: não identificada.	
9.5	**O órgão implementa o *Domain-based Message Authentication, Reporting, and Conformance* (DMARC)?**	GI2
	Implementar o protocolo DMARC por meio da implementação dos padrões *Sender Policy Framework* (SPF) e *DomainKeys Identified Mail* (DKIM), objetivando diminuir a chance de e-mails forjados.	
	Normas de referência: não identificada.	
9.6	**O órgão bloqueia tipos de arquivo desnecessários?**	GI2

	Bloquear tipos de arquivo desnecessários que tentem entrar no *gateway* de e-mail da organização.	
	Normas de referência: não identificada.	
9.7	**O órgão implementa e mantém proteções *antimalware* nos servidores de e-mail?**	**GI3**
	Implementar e manter proteção *antimalware* de servidores de e-mail, como varredura de anexos ou *sandbox*.	
	Normas de referência: não identificada.	

5.10 CONTROLE 10: Defesa contra *malware*

Visão geral

Prevenir a instalação, disseminação e execução de aplicativos, códigos ou *scripts* maliciosos em ativos institucionais.

Por que esse controle é crítico?

Software maliciosos são uma ameaça constante, com finalidades diversas como captura de credenciais, roubo e destruição de dados. O *malware* evolui usando técnicas como aprendizado de máquina para evitar ou desabilitar defesas. Ele entra nas organizações por vulnerabilidades em dispositivos de usuários finais, anexos de *e-mail*, páginas *web*, serviços em nuvem, dispositivos móveis e mídias removíveis, explorando comportamentos inseguros como clicar em *links*, abrir anexos ou usar *pen drives* USB.

As defesas contra *malware* devem operar de forma automatizada, atualizada rapidamente e integradas a processos como gerenciamento de vulnerabilidades e gestão de incidentes, sendo implantadas em todos os pontos de entrada e ativos institucionais para detectar, impedir a disseminação e controlar a execução do código malicioso.

Procedimentos e ferramentas

A proteção eficaz contra *malware* inclui suítes tradicionais de prevenção e detecção em *endpoints*, com atualizações automatizadas dos fornecedores para manter os Indicadores de Comprometimento (IOCs) atualizados. Essas ferramentas devem ser gerenciadas centralizadamente para garantir consistência em toda a infraestrutura.

Além de bloquear e identificar *malware*, este controle destaca a importância da coleta centralizada de *logs* para suportar alertas, identificação e resposta a incidentes. Invasores utilizam técnicas *Living Off The Land* (LotL), empregando recursos já existentes no ambiente para evitar detecção. Habilitar o registro em *log* facilita o acompanhamento e a compreensão dos eventos de segurança – o controle 13 apresenta medidas detalhadas nesta perspectiva.

- Para entender como os controles do PPSI aplicam-se às técnicas mais comuns de LotL, consulte: https://www.cisecurity.org/controls/resources?crc=minimize-your-threats

Lista de medidas

ID	Título, descrição e normas de referência	GI
10.1	**O órgão instala e mantém um software *antimalware*?**	**GI1**
Instalar e manter um software *antimalware* em todos os ativos institucioanais que possibilitem esta instalação.		
Normas de referência: não identificada.		
10.2	**O órgão configura atualizações automáticas de assinatura *antimalware*?**	**GI1**
Configurar atualizações automáticas para as assinaturas *antimalware* em todos os ativos institucionais que possibilitem esta configuração.		
Normas de referência: não identificada.		
10.3	**O órgão desabilita a execução e reprodução automática para mídias removíveis?**	**GI1**
Configurar os dispositivos para a não execução e reprodução automática de mídias removíveis.		
Normas de referência: não identificada.		
10.4	**O órgão configura a varredura *antimalware* automática de mídias removíveis?**	**GI2**
Configurar o software *antimalware* para verificar automaticamente mídias removíveis.		
Normas de referência: não identificada.		
10.5	**O órgão habilita funções antiexploração (*anti-exploit*)?**	**GI2**
Implantar recursos de proteção antiexploração nos ativos institucionais, sempre que possível.		
Normas de referência: não identificada.		
10.6	**O órgão gerencia o software *antimalware* de forma centralizada?**	**GI2**
Utilizar software *antimalware* gerenciado de forma centralizada.		
Normas de referência: não identificada.		
10.7	**O órgão utiliza software *antimalware* baseado em comportamento?**	**GI2**
Utilizar software *antimalware* baseado em comportamento.		
Normas de referência: não identificada.		

5.11 CONTROLE 11: Recuperação de dados

Visão geral

Estabelecer e manter práticas de realização de cópias de segurança e recuperação de dados suficientes para restaurar os ativos institucionais para um estado confiável e pré-incidente.

Por que esse controle é crítico?

Na tríade da segurança da informação – confidencialidade, integridade e disponibilidade (CID) –, a disponibilidade dos dados é, em alguns casos, tão crítica quanto a sua confidencialidade, pois dados indisponíveis ou não confiáveis impactam decisões de negócios. Além de possíveis erros humanos, invasores fazem alterações difíceis de detectar em configurações, contas e adicionam *software* e scripts maliciosos. Por isso, ter cópias de segurança ou imagens recentes é essencial para recuperar os ativos a um estado confiável.

O *ransomware*, apesar de não ser novidade, aumentou muito e evoluiu para extorsão, onde dados são exfiltrados antes da criptografia, com exigência de pagamento para evitar a divulgação. Ter cópias de segurança ajuda a restaurar sistemas, mas não evita a exposição dos dados. Seguir os demais controles CIS auxiliará na prevenção dos riscos de *ransomware* pela melhoria da higiene cibernética.

Procedimentos e ferramentas

Os procedimentos de realização de cópias de segurança e recuperação de dados devem estar relacionados com o processo de gerenciamento de dados do controle 3, incluindo *backups* baseados na criticidade dos dados para a organização e requisitos legais de retenção dos dados, determinando a frequência e o tipo de *backup* (completo ou incremental).

Trimestralmente, ou após mudanças em processos ou tecnologias, recomenda-se que uma equipe realize testes de restauração de cópias de segurança em ambiente controlado, verificando a integridade e funcionalidade do sistema operacional, soluções de *software* e dados, avaliando o tempo do processo de restauração e seu impacto em casos de necessidade.

Lista de medidas

ID	Título, descrição e normas de referência	GI
11.1	**O órgão estabelece e mantém um processo de realização de cópias de segurança (*backup*)?**	**GI1**
	Estabelecer e manter um processo de realização de cópias de segurança (*backups*), incluindo as atividades de recuperação de dados. Tal processo deve descrever em seu escopo critérios de priorização para recuperação, bem como medidas para segurança dos dados. Periodicamente, deve ser realizada uma revisão ou atualização deste processo,	

assim como em casos específicos quando ocorrerem mudanças significativas que venham a impactar esta medida.

Normas de referência: **IN GSI/PR nº 8/2025, art. 3º, VI.

11.2	O órgão executa *backups* automatizados?	GI1

Estabelecer e manter procedimentos para que todos os dados dos ativos institucionais tenham cópias de segurança (*backups*) realizadas automaticamente e de forma regular, de acordo com a criticidade dos dados.

Normas de referência: não identificada.

11.3	O órgão protege os dados de recuperação?	GI1

Estabelecer e manter procedimentos para proteger os dados de recuperação com controles equivalentes aos dos dados originais. Considerar o uso de criptografia ou separação de dados, conforme os requisitos.

Normas de referência: NC nº 20/IN01/DSIC/GSIPR, 6.2.4; IN GSI/PR nº 3/2013; NC nº 09/IN01/DSIC/GSIPR; **IN GSI/PR nº 8/2025, art. 3º, VI.

11.4	O órgão estabelece e mantém uma instância isolada de dados de recuperação?	GI1

Criar e manter pelo menos uma instância isolada dos dados de recuperação. Alguns exemplos deste tipo de implementação são o controle de versão de destinos de backup por meio de sistemas ou serviços *off-line* (*backup off-line*, não acessível por meio de uma conexão de rede), em nuvem, ou em datacenter separado do site local.

Normas de referência: não identificada.

11.5	O órgão testa a recuperação dos dados?	GI2

Realizar o teste de integridade do *backup* regularmente, executando um processo de restauração de dados para assegurar que o *backup* esteja funcionando corretamente conforme política de *backup*.

Normas de referência: NC nº 20/IN01/DSIC/GSIPR, 6.3.9; **IN GSI/PR nº 8/2025, art. 3º, VI.

** A IN GSI/PR nº 8/2025 estabelece os requisitos mínimos de segurança da informação para tratamento de informação classificada em computação em nuvem, sendo uma norma de referência apenas para estas situações.

5.12 CONTROLE 12: Gestão de infraestrutura de rede

Visão geral

Estabelecer, implementar e gerenciar ativamente (rastrear, reportar, corrigir) os ativos de rede, a fim de evitar que atacantes explorem serviços de rede e pontos de acesso vulneráveis.

Por que esse controle é crítico?

Uma infraestrutura de rede segura é essencial para a defesa contra ataques, incluindo arquitetura adequada, tratamento de vulnerabilidades introduzidas por configurações padrão, monitoramento de alterações e reavaliação das configurações. Essa infraestrutura abrange *gateways* físicos e virtualizados, *firewalls*, pontos de acesso sem fio, roteadores e *switches*.

Configurações padrão focam na facilidade de uso, não na segurança, podendo conter serviços e portas abertas, contas e senhas padrão, protocolos vulneráveis e soluções de *software* desnecessárias. Invasores exploram essas vulnerabilidades e inconsistências em regras de *firewall*, roteadores e *switches* para acessar redes, redirecionar tráfego e interceptar dados.

A segurança de rede exige reavaliações regulares de arquitetura, configurações, controles de acesso e fluxos de tráfego, pois as vulnerabilidades de segurança podem surgir a partir de exceções comerciais que não são removidas ou analisadas adequadamente ao longo do tempo.

Procedimentos e ferramentas

As organizações devem garantir documentação completa da infraestrutura de rede e manter diagramas de arquitetura atualizados, incluindo arquitetura de segurança. Os componentes devem ter suporte para *patches* e atualizações, sendo substituídos antes do fim de vida (*End of Line*, EOL) ou isolados por controles de mitigação. Dessa forma, é necessário monitorar versões e configurações para identificar vulnerabilidades e atualizar dispositivos de rede para versões seguras e estáveis sem impactar a infraestrutura.

É necessário ter gerenciamento completo de contas para controle de acesso, registro e monitoramento, com administração da infraestrutura realizada por meio de protocolos seguros, autenticação forte (MFA para PAM, *Privileged Access Management*) e a partir de dispositivos ou redes dedicadas.

Ferramentas comerciais podem automatizar a avaliação de regras de filtragem de rede, detectando inconsistências ou erros em conjuntos de regras e Listas de Controle de Acesso (*Access Control Lists*, ACLs), e devem ser usadas após alterações significativas nessas regras.

- Para obter orientações sobre teletrabalho e pequenos escritórios, consulte o Guia de Segurança de Rede para Teletrabalho e Pequenos Escritórios do CIS *Controls*, consulte: https://www.cisecurity.org/controls/resources?crc=environment-specific-guidance

Lista de medidas

ID	Título, descrição e normas de referência	GI
12.1	**O órgão mantém atualizada a infraestrutura de rede?**	GI1
	Estabelecer e manter procedimentos para assegurar que a infraestrutura de rede da organização esteja sempre atualizada. Revisar as versões de *software* mensalmente, ou	

com maior frequência, para verificar se ainda estão sendo suportados pelos seus fornecedores.

Normas de referência: não identificada.

12.2	**O órgão estabelece e mantém uma arquitetura de rede segura?**	**GI2**

Projetar e manter uma arquitetura de rede segura abordando, no mínimo, segmentação, privilégio mínimo e disponibilidade. Exemplos de implementações incluem documentação, políticas e componentes de projeto.

Normas de referência: *IN GSI/PR nº 5/2021, art. 15; **IN GSI/PR nº 8/2025, art. 3º, I, II, III.

12.3	**O órgão gerencia a infraestrutura de rede com segurança?**	**GI2**

Gerenciar com segurança a infraestrutura de rede da organização. Exemplos de implementações incluem a Infraestrutura como Código (*Infrastructure as Code*, IaC) com controle de versão e o uso de protocolos de rede seguros.

Normas de referência: não identificada.

12.4	**O órgão elabora e mantém diagramas de arquitetura?**	**GI2**

Elaborar e manter diagramas e demais documentações da arquitetura de rede da organização. Revisar e atualizar as documentações anualmente ou quando ocorrerem mudanças significativas que possam impactar esta medida.

Normas de referência: não identificada.

12.5	**O órgão centraliza a autenticação, a autorização e a auditoria (*Authentication, Authorization, and Accounting*, AAA) de rede?**	**GI2**

Centralizar a autenticação, autorização e auditoria da rede.

Normas de referência: não identificada.

12.6	**O órgão utiliza protocolos seguros de comunicação e gerenciamento de rede?**	**GI2**

Adotar protocolos de comunicação e gerenciamento de rede seguros.

Normas de referência: não identificada.

12.7	**O órgão assegura que os dispositivos remotos utilizem uma Rede Privada Virtual (*Virtual Private Network*, VPN) e se conectam em uma infraestrutura de autenticação, autorização e auditoria (*Authentication, Authorization, and Accounting*, AAA)?**	**GI2**

Exigir que os usuários que acessam a rede de forma remota utilizem uma VPN gerenciada pela organização e realizem autenticação via serviços AAA antes de qualquer acesso.

Normas de referência: não identificada.

12.8	O órgão utiliza e mantém recursos computacionais dedicados para todas as atividades administrativas de TI?	GI3

Estabelecer e manter recursos de computação dedicados, física ou logicamente separados, para todas as tarefas administrativas de TI ou tarefas que exijam acesso administrativo. Os recursos de computação devem ser segmentados da rede primária da organização e não devem ter acesso à internet.

Normas de referência: não identificada.

* A IN GSI/PR nº 5/2021 estabelece os requisitos mínimos de segurança da informação para que órgãos e entidades da administração pública federal utilizem soluções de computação em nuvem, sendo uma norma de referência apenas para estes ambientes computacionais.
** A IN GSI/PR nº 8/2025 estabelece os requisitos mínimos de segurança da informação para tratamento de informação classificada em computação em nuvem, sendo uma norma de referência apenas para estas situações.

5.13 CONTROLE 13: Monitoramento e defesa de rede

Visão geral

Implementar processos e ferramentas para estabelecer e manter monitoramento abrangente de rede e defesa contra ameaças de segurança em toda a infraestrutura de rede e base de usuários da organização.

Por que esse controle é crítico?

Mesmo que as defesas de rede funcionem e auxiliem na mitigação de riscos, elas não são perfeitas, sendo necessário compreender a postura de risco da organização para configurá-las, ajustá-las e registrá-las corretamente. Configurações incorretas devido a erro humano ou desconhecimento dos recursos das ferramentas podem gerar falsa sensação de segurança.

Ferramentas de segurança são eficazes apenas com monitoramento contínuo que alerte e permita resposta rápida a incidentes, envolvendo visibilidade total dos vetores de ataque e o uso de humanos no processo de detecção, análise e resposta. Grandes organizações ou aquelas fortemente visadas devem ter operações de segurança para prevenir, detectar e responder rapidamente, gerando relatórios e métricas que aprimoram políticas e promovam a conformidade regulatória.

A consciência situacional – capacidade de perceber, compreender e antecipar elementos e riscos no ambiente em um dado espaço-tempo, permitindo tomada de decisão rápida e eficaz – tem como principal benefício aumentar a velocidade de detecção e resposta, reduzindo o impacto de *malware*, roubo de credenciais ou comprometimento de dados. Por meio dela, organizações catalogam Táticas, Técnicas e Procedimentos (TTPs) e IOCs, permitindo uma abordagem mais proativa e recuperação mais rápida com informações completas para estratégias eficientes.

Procedimentos e ferramentas

A consciência situacional não exige necessariamente um Centro de Operações de Segurança (*Security Operations Center*, SOC) e começa com o entendimento das funções críticas, arquiteturas, dados, serviços de fornecedores e demais ativos institucionais da organização. Isso é a base para criação de uma arquitetura de segurança, aplicação de medidas técnicas, registro de eventos de segurança, monitoramento e procedimentos de resposta, conduzidos por uma equipe treinada, internamente ou por terceiros.

A tecnologia é fundamental para coletar e analisar dados, monitorando redes e demais ativos internos e externos, incluindo plataformas em nuvem. Encaminhar eventos de segurança para soluções de Gerenciamento de Eventos e Informações de Segurança (*Security Information and Event Management*, SIEM) e ferramentas de correlação de eventos pode agregar valor, mas não é suficiente para oferecer uma visão completa. Essas ferramentas não substituem profissionais qualificados, essenciais para detectar e entender ataques e promover a implantação adequada e ajustes necessários nessas soluções.

Com a maturidade do processo, a organização desenvolverá uma base de conhecimento para avaliar riscos, construindo capacidade interna de inteligência contra ameaças e coletando TTPs de adversários. Algumas organizações maduras podem avançar para caça às ameaças, revisando manualmente *logs*, fluxos de dados e tráfego para identificar anomalias.

Lista de medidas

ID	Título, descrição e normas de referência	GI
13.1	**O órgão centraliza alertas de eventos de segurança?**	**GI2**
Centralizar os alertas de eventos de segurança dos ativos institucionais e soluções de software da organização para correlação e análise de registros. As boas práticas demandam o uso de um *Security Information and Event Management* (SIEM), que inclui alertas de correlação de eventos definidos pelo fornecedor. Uma plataforma de análise de log configurada com aletas de correlação relevantes para a segurança também atende esta medida.		
Normas de referência: NC nº 21/IN01/DSIC/GSIPR, 6.8; **IN GSI/PR nº 8/2025, art. 3º, X.		
13.2	**O órgão implanta soluções de detecção de intrusão baseada em *host*?**	**GI2**
Implantar soluções para detecção de intrusão baseada em *host* nos ativos institucionais, quando apropriado ou suportado.		
Normas de referência: não identificada.		
13.3	**O órgão implanta soluções de detecção de intrusão de rede?**	**GI2**
Implantar soluções para detecção de intrusão de rede nos ativos institucionais, quando apropriado. Exemplos de implementações incluem o uso de um *Network Intrusion Detection System* (NIDS) ou serviço de provedor de nuvem equivalente.		

Normas de referência: não identificada.

13.4	O órgão realiza filtragem de tráfego entre os segmentos de rede?	GI2

Realizar a filtragem de tráfego entre os segmentos de rede, quando apropriado.

Normas de referência: não identificada.

13.5	O órgão realiza o gerenciamento de controle de acesso para ativos remotos?	GI2

Gerenciar o controle de acesso em ativos institucionais que se conectam remotamente aos recursos da organização. Determinar a quantidade de acesso aos recursos organizacionais com base em: *software antimalware* instalados e atualizados, conformidade com o processo de configuração segura dos ativos institucionais e garantia de que os sistemas operacionais e demais aplicações estejam atualizados.

Normas de referência: não identificada.

13.6	O órgão coleta *logs* de fluxo de tráfego de rede?	GI2

Realizar a coleta dos *logs* de fluxo de tráfego de rede com o objetivo de checar e alertar sobre dispositivos de rede que estejam com comportamento suspeito relacionado às suas necessidades de acesso para execução de suas funcionalidades.

Normas de referência: não identificada.

13.7	O órgão implanta soluções para prevenção de intrusão baseada em *host*?	GI3

Implantar uma solução de prevenção de intrusão baseada em *host* nos ativos institucionais, quando suportado. Exemplos de implementações incluem o uso de um cliente *Endpoint Detection and Response* (EDR) ou de um agente *Instrusion Prevention System* (IPS) baseado em *host*.

Normas de referência: não identificada.

13.8	O órgão implanta soluções para prevenção de intrusão de rede?	GI3

Implantar uma solução para prevenção de intrusão baseada em rede, quando suportado. Exemplos de implementações incluem o uso de um sistema de prevenção de intrusão de rede (*Network Intrusion Prevention System*, NIPS) ou serviço de provedor de nuvem equivalente.

Normas de referência: não identificada.

13.9	O órgão implanta controle de acesso em nível de porta?	GI3

Implantar o controle de acesso em nível de porta. Esta medida utiliza o protocolo 802.1x ou soluções semelhantes como certificados, e pode incorporar a autenticação de usuário ou dispositivo.

Normas de referência: não identificada.

13.10 O órgão realiza a filtragem da camada de aplicação?	GI3

Realizar a filtragem da camada de aplicação. Exemplos de implementações incluem um *proxy* de filtragem, *firewall* da camada de aplicação ou *gateway*.

Normas de referência: não identificada.

13.11 O órgão ajusta limites de alertas de eventos de segurança?	GI3

Ajustar periodicamente os limites dos alertas de eventos de segurança para assegurar a eficácia na detecção de ameaças.

Normas de referência: não identificada.

** A IN GSI/PR nº 8/2025 estabelece os requisitos mínimos de segurança da informação para tratamento de informação classificada em computação em nuvem, sendo uma norma de referência apenas para estas situações.

5.14 CONTROLE 14: Conscientização e treinamento de competências

Visão geral

Estabelecer e manter ações de treinamento e um programa de conscientização em segurança da informação contínuo para influenciar o comportamento dos agentes públicos, tornando-os qualificados e conscientes para reduzir os riscos de segurança da informação para a organização.

Por que esse controle é crítico?

As ações dos agentes públicos são fundamentais para o sucesso do aprimoramento da maturidade em segurança da informação nas organizações. É mais fácil para um invasor induzir um usuário a clicar em um *link* ou abrir um anexo de *e-mail* do que explorar diretamente uma vulnerabilidade de rede.

Usuários, intencionalmente ou não, podem causar incidentes por manuseio incorreto de dados críticos para a organização, envio errado de *e-mails*, perda de dispositivos, uso de senhas fracas ou repetidas em sites públicos.

Nenhum programa de segurança é eficaz sem abordar o fator humano, considerando que diferentes níveis e funções na organização apresentam riscos variados, como executivos com dados mais críticos e administradores com acesso privilegiado.

Dessa forma, a implementação de um programa de conscientização sobre segurança da informação contínuo, e sua atualização regular, são essenciais para fortalecer a cultura de segurança e reduzir práticas arriscadas.

Procedimentos e ferramentas

Um programa eficaz de conscientização em segurança da informação vai além do treinamento anual com vídeos e testes de *phishing*, incluindo mensagens frequentes e atualizadas sobre temas relevantes, como uso de senhas fortes e campanhas de *phishing* sazonais.

O programa de conscientização deve considerar requisitos regulatórios e ameaças específicas da organização, além de abranger diferentes funções, como tentativas de comprometimento de caixas de *e-mail* (*Business Email Compromise,* BEC) para a equipe financeira, simulando pedidos fraudulentos de transferência ou alteração de dados bancários.

Para uma abordagem mais abrangente deste tópico, e a construção de um programa eficaz de conscientização sobre segurança da informação, os seguintes recursos são úteis:

- materiais educativos disponibilizados pelo Centro de Excelência em Privacidade e Segurança (CEPS GOV.BR): https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/centro-de-excelencia-em-privacidade-e-seguranca
- NIST® SP 800-50 - Construindo um Programa de Aprendizagem em Segurança Cibernética e Privacidade: https://csrc.nist.gov/pubs/sp/800/50/r1/final
- Centro Nacional de Segurança Cibernética (Reino Unido): https://www.ncsc.gov.uk/guidance/10-steps-user-education-and-awareness
- EDUCAUSE: https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/awareness-campaigns
- Aliança Nacional de Segurança Cibernética (NCSA): https://staysafeonline.org/
- SANS: https://www.sans.org/security-awareness-training/resources

Lista de medidas

ID	Título, descrição e normas de referência	GI
14.1	**O órgão implementa um programa de conscientização em segurança da informação?**	**GI1**
Estabelecer e manter um programa de conscientização em segurança da informação com o objetivo de promover tal cultura na organização, conscientizar seus agentes públicos sobre responsabilidades e procedimentos relacionados ao tema e sobre como interagir com ativos institucionais de forma segura. Prever procedimentos de conscientização no ingresso dos agentes públicos e de forma continuada, de acordo com a NC nº 18/IN01/DSIC/GSIPR. Revisar e atualizar o conteúdo do programa anualmente ou quando ocorrerem mudanças significativas na organização que possam impactar esta medida.		
Normas de referência: NC nº 18/IN01/DSIC/GSIPR; Decreto nº 12.572/2025, art. 10, V; IN GSI/PR nº 1/2020, art. 19, II.		
14.2	**O órgão conscientiza os agentes públicos para reconhecer ataques de engenharia social?**	**GI1**

Garantir que o programa de conscientização contemple conteúdo sobre como identificar diferentes formas de ataques de engenharia social, como *phishing*, comprometimento de e-mail institucional, golpes de telefone e chamadas realizadas por impostores.

Normas de referência: NC nº 18/IN01/DSIC/GSIPR; Decreto nº 12.572/2025, art. 10, V; IN GSI/PR nº 1/2020, art. 19, II.

14.3	**O órgão conscientiza os agentes públicos nas melhores práticas de autenticação?**	**GI1**

Garantir que o programa de conscientização contemple conteúdo sobre as melhores práticas de autenticação. Exemplos de tópicos incluem autenticação multifator (*Multi-Factor Authentication*, MFA), composição de senhas e gerenciamento de credenciais.

Normas de referência: NC nº 18/IN01/DSIC/GSIPR; Decreto nº 12.572/2025, art. 10, V; IN GSI/PR nº 1/2020, art. 19, II.

14.4	**O órgão conscientiza os agentes públicos nas melhores práticas de tratamento de dados?**	**GI1**

Garantir que o programa de conscientização contemple conteúdo sobre como identificar e armazenar, transferir, arquivar e destruir adequadamente informações. Isto também inclui conscientizar sobre práticas recomendadas de mesa e tela limpas (não deixar senhas expostas nas mesas de trabalho e bloquear a tela da estação de trabalho ao se ausentar), apagar quadros físicos e virtuais após reuniões e tratar dados e demais ativos institucionais com segurança.

Normas de referência: NC nº 18/IN01/DSIC/GSIPR; NC nº 20/IN01/DSIC/GSIPR, item 4.7; Decreto nº 12.572/2025, art. 10, V; IN GSI/PR nº 1/2020, art. 19, II.

14.5	**O órgão conscientiza os agentes públicos sobre as causas ocorrências não intencionais que podem expor dados?**	**GI1**

Garantir que o programa de conscientização contemple conteúdo sobre ocorrências não intencionais de exposição de dados, como entrega incorreta de dados pessoais, sigilosos ou com alguma restrição de acesso, perda de dispositivos móveis ou publicação de dados não intencional.

Normas de referência: NC nº 18/IN01/DSIC/GSIPR; Decreto nº 12.572/2025, art. 10, V; IN GSI/PR nº 1/2020, art. 19, II.

14.6	**O órgão conscientiza os agentes públicos sobre como reconhecer e notificar incidentes de segurança da informação?**	**GI1**

Garantir que o programa de conscientização contemple conteúdo que oriente os agentes públicos para serem capazes de identificar os indicadores mais comuns de um incidente e serem capazes de notificar tal incidente.

Normas de referência: NC nº 18/IN01/DSIC/GSIPR; Decreto nº 12.572/2025, art. 10, V; IN GSI/PR nº 1/2020, art. 19, II.

14.7	**O órgão conscientiza os agentes públicos sobre como identificar e comunicar se os ativos institucionais estão sem atualizações de segurança?**	**GI1**

Garantir que o programa de conscientização contemple conteúdo sobre verificar e notificar desatualizações ou quaisquer falhas em ferramentas e processos automatizados.

Normas de referência: NC nº 18/IN01/DSIC/GSIPR; Decreto nº 12.572/2025, art. 10, V; IN GSI/PR nº 1/2020, art. 19, II.

14.8	**O órgão conscientiza os agentes públicos sobre os perigos de se conectar e transmitir dados organizacionais em redes inseguras?**	**GI1**

Garantir que o programa de conscientização contemple conteúdo sobre os riscos de se conectar e transmitir dados em redes inseguras para atividades da organização. Se a organização tiver agentes públicos em teletrabalho, é relevante incluir no programa de conscientização recomendações sobre configuração segura da infraestrutura de rede doméstica do agente público.

Normas de referência: NC nº 18/IN01/DSIC/GSIPR; Decreto nº 12.572/2025, art. 10, V; IN GSI/PR nº 1/2020, art. 19, II.

14.9	**O órgão implementa ações para capacitação sobre segurança da informação?**	**GI2**

Incluir nos instrumentos de capacitação de pessoas da organização, a exemplo do Plano de Desenvolvimento de Pessoas, as necessidades de treinamento em segurança da informação para agentes públicos que atuem em funções específicas, de modo a atender suas competências específicas, e promover a execução de tais instrumentos. Exemplos de necessidades de capacitação incluem cursos de desenvolvimento de software seguro para profissionais de TI, prevenção de vulnerabilidades para desenvolvedores de aplicações da web, acesso e utilização dos registros gerados por provedores de serviço de nuvem e treinamento avançado sobre engenharia social para funções de níveis estratégico da organização. Considerar as NC nº 17/IN01/DSIC/GSIPR e NC nº 18/IN01/DSIC/GSIPR.

Normas de referência: NC nº 17/IN01/DSIC/GSIPR; NC nº 18/IN01/DSIC/GSIPR; *IN GSI/PR nº 5/2021, art. 13, VII e art. 16, I; Decreto nº 12.572/2025, art. 3º, IV, art. 4º, VI e art. 10, V; IN GSI/PR nº 1/2020, art. 19, II.

* A IN GSI/PR nº 5/2021 estabelece os requisitos mínimos de segurança da informação para que órgãos e entidades da administração pública federal utilizem soluções de computação em nuvem, sendo uma norma de referência apenas para estes ambientes computacionais.

5.15 CONTROLE 15: Gestão de provedor de serviços

Visão geral

Desenvolver um processo para avaliar provedores de serviços que detêm dados críticos para a organização ou são responsáveis por plataformas ou processos críticos de TI do órgão, a fim de garantir que esses provedores estejam protegendo essas plataformas e dados adequadamente.

Por que esse controle é crítico?

As organizações dependem de fornecedores e parceiros para gerenciar dados e infraestrutura essencial. Violações em terceiros já causaram impactos significativos, como comprometimento de cartões de pagamento por invasores em provedores menores e ataques de *ransomware* que interrompem negócios, podendo afetar diretamente a organização principal.

Regulamentações exigem que a proteção de dados se estenda aos provedores de serviços, como a *Health Insurance Portability and Accountability Act* (HIPAA), *Federal Financial Institutions Examination Council* (FFIEC) e os Fundamentos Cibernéticos do Reino Unido, tornando a gestão de riscos de terceiros parte essencial da Governança, Risco e Conformidade (GRC), pois riscos não gerenciados internamente são transferidos a entidades externas.

Na Administração Pública federal direta, autárquica e fundacional há diversas regulamentações aplicáveis às contratações. Nesse contexto, esses instrumentos foram especificados nas normas de referência correspondentes a cada medida deste controle, devendo ser avaliados para garantir a correta implementação das ações.

Apesar da longa prática de revisão das medidas de segurança da informação aplicadas por terceiros contratados, não há padrão universal para avaliação, o que leva a auditorias frequentes e variadas que impactam a produtividade dos provedores.

Organizações menores geralmente representam riscos maiores que grandes fornecedores de serviços críticos, especialmente porque estes podem subcontratar terceiros adicionais para fornecer *plugins* ou serviços que suportam a oferta principal.

Procedimentos e ferramentas

A maioria das organizações usa listas de verificação padrão, como ISO 27001 ou Controles CIS, muitas vezes gerenciadas por planilhas, embora plataformas online para gestão centralizada estejam disponíveis. Plataformas para gestão de provedores oferecem inventários e pontuações dinâmicas de risco baseadas em avaliações técnicas passivas ou enriquecidas por outras organizações, auxiliando decisões mais informadas.

O foco deste Controle CIS é no processo em si, que deve ser revisado anualmente, pois relacionamentos e dados podem mudar. Independentemente do porte, a organização deve ter política de revisão de prestadores, inventário atualizado deles e classificação de risco conforme o impacto potencial nos negócios, incluindo cláusulas contratuais de responsabilização por

incidentes. Provedores com contrato de segurança gerenciada, garantias e seguro cibernético ajudam a reduzir riscos.

Ao encerrar contratos, é fundamental realizar desativação segura dos provedores, como desativar contas, encerrar fluxos de dados e promover o descarte seguro de dados nos sistemas do provedor de serviços.

Lista de medidas

ID	Título, descrição e normas de referência	GI
15.1	**O órgão estabelece e mantém o inventário de provedores de serviços?**	GI1
	Estabelecer e manter o inventário de provedores de serviços que mantêm dados críticos ou são responsáveis por plataformas ou processos de TI relevantes para a organização. Este inventário deve incluir as classificações dos provedores, conforme medida 15.3, e conter seus contatos institucionais. Revisar e atualizar o inventário anualmente ou quando ocorrerem mudanças significativas do provedor que venham impactar a organização de forma significativa.	
	Normas de referência: IN GSI/PR nº 3/2021, Capítulo II	
15.2	**O órgão estabelece e mantém uma política de gestão de provedores de serviços?**	GI2
	Estabelecer e manter uma política de gestão de provedores de serviços. Certifique-se de que a política aborde o inventário, a categorização, a avaliação, o monitoramento e o encerramento da operação dos provedores de serviços. Revisar e atualizar a política anualmente ou quando ocorrerem mudanças significativas na organização que possam afetar esta medida.	
	Normas de referência: IN SGD/ME nº 94/2022; *IN GSI/PR nº 5/2021; **IN GSI/PR nº 8/2025.	
15.3	**O órgão categoriza provedores de serviços?**	GI2
	Categorizar os provedores de serviços considerando características tais como: criticidade dos dados que trata, volume de dados, requisitos de disponibilidade, normas aplicáveis, risco inerente e risco residual. Revisar e atualizar as categorizações anualmente ou quando ocorrerem mudanças significativas na organização que possam afetar esta medida.	
	Normas de referência: *IN GSI/PR nº 5/2021, art. 3º, art. 11, III, IV, V, art. 17 e art. 18; Portaria SGD/MGI nº 5.950/2023.	
15.4	**O órgão descreve os requisitos mínimos de segurança da informação nos contratos dos provedores de serviços?**	GI2
	Inserir cláusulas nos contratos dos provedores de serviços que contenham requisitos de segurança da informação. Requisitos como segurança do software, resposta a incidentes de	

segurança, criptografia, descarte de dados, entre outros, devem ser abordadas. Tais requisitos mínimos devem ser concisos e estar de acordo com a política de gestão de provedores de serviços da organização. Revisar os contratos de provedores de forma periódica com o objetivo de atualizar e assegurar que os requisitos estão sendo cumpridos.

Normas de referência: IN SGD/ME nº 94/2022; Portaria SGD/MGI nº 5.950/2023; Portarias SGD/MGI nº 750/2023 e nº 6.679/2024; Portarias SGD/MGI nº 1.070/2023 e nº 6.680/2024; Portaria SGD/MGI nº 2.715/2023; Portaria SGD/MGI nº 370/2023; *IN GSI/PR nº 5/2021, arts. 16, II e III, 19, 22, 23 e 25; **IN GSI/PR nº 8/2025.

15.5	O órgão avalia provedores de serviços?	GI3

Avaliar os provedores de serviços de acordo com a política de gestão de provedores de serviços da organização. O escopo da avaliação pode variar de acordo com as classificações, podendo ser realizada por meio da análise de relatórios de avaliação padronizados, aplicação de questionários, processos rigorosos aplicáveis, entre outros. A avaliação de provedores de serviço deve ser realizada de forma periódica e na medida em que novos contratos forem estipulados ou renovados.

Normas de referência: IN SGD/ME nº 94/2022; Portaria SGD/MGI nº 5.950/2023; Portarias SGD/MGI nº 750/2023 e nº 6.679/2024; Portarias SGD/MGI nº 1.070/2023 e nº 6.680/2024; Portaria SGD/MGI nº 2.715/2023; Portaria SGD/MGI nº 370/2023; *IN GSI/PR nº 5/2021, art. 20; **IN GSI/PR nº 8/2025, arts. 7º, 8º, 9º e 10.

15.6	O órgão monitora provedores de serviço?	GI3

Realizar o monitoramento dos provedores de acordo com a política de gestão de provedores de serviços da organização. O monitoramento pode incluir a reavaliação periódica de conformidade do provedor, avaliação de artefatos entregues pelo provedor e monitoramento na dark web.

Normas de referência: IN SGD/ME nº 94/2022; Portarias SGD/MGI nº 750/2023 e nº 6.679/2024; Portarias SGD/MGI nº 1.070/2023 e nº 6.680/2024; Portaria SGD/MGI nº 2.715/2023; Portaria SGD/MGI nº 5.950/2023; Portaria SGD/MGI nº 370/2023.

15.7	O órgão encerra de forma segura o contrato com o provedor de serviços?	GI3

Realizar de forma segura o encerramento de contrato de provedores e prestadores de serviço. Algumas ações que podem ser utilizadas para encerrar os contratos ou desligar os prestadores são: desativação de contas de usuário e serviço utilizados durante o contrato, encerramento de fluxo de dados e descarte seguros de dados e informações corporativas em sistemas dos provedores de serviço.

Normas de referência: IN SGD/ME nº 94/2022; Portaria SGD/MGI nº 5.950/2023; *IN GSI/PR nº 5/2021, art. 19, V e VI.

* A IN GSI/PR nº 5/2021 estabelece os requisitos mínimos de segurança da informação para que órgãos e entidades da administração pública federal utilizem soluções de computação em nuvem, sendo uma norma de referência apenas para estes ambientes computacionais.
** A IN GSI/PR nº 8/2025 estabelece os requisitos mínimos de segurança da informação para tratamento de informação classificada em computação em nuvem, sendo uma norma de referência apenas para estas situações.

5.16 CONTROLE 16: Segurança de aplicações

Visão geral

Gerenciar o ciclo de vida de segurança de todas as soluções de *software* desenvolvidas, hospedadas ou adquiridas internamente, com o objetivo de prevenir, detectar e corrigir vulnerabilidades de segurança antes que elas possam impactar a organização.

Por que esse controle é crítico?

Soluções de *software* permitem que usuários acessem e gerenciem dados de forma alinhada às funções de negócios, reduzindo a necessidade de interagir com funções complexas de sistemas, como acessar e manipular bancos de dados diretamente. Como estas soluções são usadas para gerenciar dados críticos e controlar acessos, podem ser exploradas por invasores para comprometer informações. Por isso, proteger as credenciais dos usuários – conforme medidas previstas no Controle 6 –, especialmente as de soluções de *software*, é fundamental.

Vulnerabilidades em soluções de *software* estão entre os vetores de ataques preferidos pelos atacantes. Soluções de *software* modernas são complexas, executadas em múltiplas plataformas e frequentemente desenvolvidas com ciclos DevOps curtos, usando combinações de *frameworks*, bibliotecas e código existente. As vulnerabilidades surgem por concepção insegura das soluções, infraestrutura vulnerável, erros de codificação, autenticação fraca e testes insuficientes. Invasores exploram falhas como estouros de *buffer*, injeção de SQL, *Cross-Site Scripting* (XSS) e outras para acessar dados ou controlar ativos vulneráveis, podendo também usar tecnologias para coletar credenciais ou instalar malware.

O uso crescente de *Software* como Serviço (SaaS), desenvolvidas e gerenciadas por terceiros em qualquer lugar do mundo, traz desafios à visibilidade sobre práticas de desenvolvimento de *software* seguro para as organizações, que precisam saber quais riscos estão assumindo ao usar essas plataformas.

Procedimentos e ferramentas

Para a Versão 8, o CIS fez parceria com o *SAFECode* objetivando desenvolver os procedimentos e medidas deste controle, focando nas ações mais críticas. Essas ações baseiam-se em um artigo complementar do *SAFECode* (referenciado nos recursos complementares ao final desta subseção), que oferece uma abordagem aprofundada.

O *SAFECode* criou uma abordagem em três níveis para ajudar a identificar o Grupo de Desenvolvimento (GD) conforme maturidade de programas, inspirada nos três níveis dos grupos de implementação do CIS usados neste guia.

- Grupo de Desenvolvimento 1: a organização depende em grande parte de *software* pronto ou de código aberto e pacotes com apenas algumas adições ocasionais de pequenas soluções de *software* ou códigos para sites. A organização é capaz de aplicar boas práticas operacionais e processuais básicas e de gerenciar a segurança das soluções de *software* fornecidas por terceiros seguindo as orientações dos Controles CIS;
- Grupo de Desenvolvimento 2: a organização utiliza algumas soluções de *software* personalizadas, desenvolvidas internamente ou por contratados, integradas a componentes de terceiros, operando tanto localmente quanto na nuvem. Conta com uma equipe de desenvolvimento que adota as melhores práticas em desenvolvimento de *software* e dedica atenção especial à qualidade e à manutenção do código terceirizado, seja ele de código aberto ou comercial, do qual depende;
- Grupo de Desenvolvimento 3: a organização investe significativamente em soluções de *software* personalizadas para suas operações, hospedadas localmente, na nuvem, ou ambos, integrando diversos componentes de código aberto e comerciais. Fornecedores de *software* e organizações que entregam SaaS devem seguir, no mínimo, os requisitos do Grupo de Desenvolvimento 3.

O primeiro passo para um programa de segurança de soluções de *software* é implementar um processo de gerenciamento de vulnerabilidades integrado ao ciclo de desenvolvimento, incluindo análise de causa raiz para corrigir falhas e priorização por severidade das remediações.

Desenvolvedores devem ser treinados em segurança de soluções de *software* e práticas de codificação segura, incluindo avaliação de *software*, módulos e bibliotecas de terceiros, para garantir que não introduzam falhas. Devem saber quais componentes usar com segurança e quais desenvolver internamente.

Vulnerabilidades na infraestrutura que suporta as soluções de *software* também geram riscos; os controles propostos no *framework* do PPSI 2.0 e a minimização da superfície de ataque ajudam a proteger redes, sistemas e contas (controles 1-7, 12 e 13).

O programa ideal integra segurança desde o início do ciclo de desenvolvimento, unificando o gerenciamento de vulnerabilidades de segurança com o processo padrão de correção de *bugs*. Equipes maiores devem adotar a modelagem de ameaças na fase de concepção para identificar falhas graves antes da codificação.

Equipes maduras podem usar programas de recompensa por *bugs* para complementar a segurança interna, identificando vulnerabilidades críticas.

Em 2020, o NIST publicou o *Secure Software Development Framework* (SSDF), consolidando melhores práticas para planejamento e avaliação da segurança de soluções de *software*, que

pode ser usado para estabelecer requisitos e avaliar processos de desenvolvimento de fornecedores.

Estes são alguns recursos sobre segurança de soluções de *software*:

- SAFECode - Adendo de segurança de soluções de software e os controles CIS: https://safecode.org/resource-publications/cis-controls/
- NIST® SP 800-218 - *Framework* de Desenvolvimento de Software Seguro (*Secure Software Development Framework*, SSDF): Recomendações para Mitigar o Risco de Vulnerabilidades de Software: https://csrc.nist.gov/pubs/sp/800/218/final
- *Business Software Alliance* - BSA *Framework* para Software Seguro: https://www.bsa.org/reports/updated-bsa-framework-for-secure-software
- Projeto Aberto de Segurança em Aplicações Web *(Open Worldwide Application Security Project*, OWASP): https://owasp.org/

Lista de medidas

ID	Título, descrição e normas de referência	GI
16.1	**O órgão estabelece e mantém um processo de desenvolvimento seguro de aplicações?**	**GI2**
Estabelecer e manter um processo de desenvolvimento seguro de aplicações. O processo deve abordar itens como: padrões de design de aplicações seguras, *privacy by design*, práticas de codificação seguras, treinamento de desenvolvedor, gerenciamento de vulnerabilidade, segurança de código de terceiros e procedimentos de teste de segurança de aplicativo. Revisar e atualizar a documentação anualmente ou quando ocorrerem mudanças institucionais significativas que possam impactar esta medida.		
Normas de referência: não identificada.		
16.2	**O órgão estabelece e mantém um processo para aceitar e tratar vulnerabilidades de software?**	**GI2**
Estabelecer e manter um processo para receber e endereçar notificações de vulnerabilidades de software, incluindo mecanismos para recebimento de notificações pela Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR). Recomenda-se que este processo esteja alinhado com processo de gestão de vulnerabilidades organizacional e inclua itens como: critérios para aceitação de vulnerabilidades identificadas e notificadas, equipe ou profissional responsável por analisar os relatórios de vulnerabilidade e um processo de entrada, atribuição, correção e testes de correção. Como parte deste processo, é importante rastrear as vulnerabilidades, classificar a gravidade e atribuir métricas capazes de medir o tempo de identificação, análise e correção das vulnerabilidades. Deve ser realizada uma revisão e alteração deste processo periodicamente, em casos específicos ou quando ocorrerem mudanças na organização que venham impactá-la de forma significativa.		

Normas de referência: não identificada.

16.3	O órgão executa análise de causa raiz em vulnerabilidades de segurança?	GI2

Executar a análise de causa raiz em vulnerabilidades de segurança. A análise da causa raiz é a tarefa capaz de avaliar os problemas subjacentes que criam vulnerabilidades no código da aplicação, e permite que as equipes de desenvolvimento, para além de atuarem apenas na vulnerabilidade, corrijam a causa raiz.

Normas de referência: não identificada.

16.4	O órgão estabelece e gerencia um inventário de componentes de software de terceiros?	GI2

Estabelecer e manter um inventário atualizado de componentes de software de terceiros usados no desenvolvimento e de componentes programados para uso futuro. Este inventário deve incluir quaisquer riscos que cada componente de terceiros possa representar para a organização. Deve ser realizada uma revisão e alteração deste inventário periodicamente, com o objetivo de identificar quaisquer mudanças ou atualizações nesses componentes e validar a compatibilidade destas.

Normas de referência: IN GSI/PR nº 3/2021, Capítulo II.

16.5	O órgão usa componentes de software de terceiros atualizados e confiáveis?	GI2

Utilizar apenas componentes de terceiros atualizados e confiáveis. Quando possível, escolher bibliotecas e estruturas pré-estabelecidas e comprovadas que forneçam a segurança adequada. É importante adquirir tais componentes de fornecedores e fontes confiáveis ou realizar a avaliação de vulnerabilidades do software antes de utilizá-las.

Normas de referência: não identificada.

16.6	O órgão estabelece e mantém um sistema e processos para a classificação de severidade de vulnerabilidades de aplicações?	GI2

Estabelecer e manter um processo para a classificação do grau de severidade das vulnerabilidades de aplicações, capaz de facilitar a priorização à medida que as vulnerabilidades descobertas são corrigidas. Este processo deve incluir a definição de um nível mínimo de aceitabilidade de segurança para a liberação de código ou aplicações. A classificação da severidade deve trazer uma forma sistemática de triagem de vulnerabilidades que venha a melhorar a gestão de riscos e assegurar que os bugs mais graves sejam priorizados. Revisar o processo o e a classificação de vulnerabilidades periodicamente.

Normas de referência: não identificada.

16.7	O órgão usa modelos de configurações de proteção padrão para infraestrutura de aplicações?	GI2

Adotar configurações de segurança padronizadas para todos os componentes da infraestrutura de aplicações, incluindo servidores, bancos de dados, servidores web, contêineres, e serviços baseados em Plataforma como Serviço (*Platform as a Service*, PaaS) e componentes de Software como Serviço (*Software as a Service*, SaaS). A organização deve adotar configurações de padrões reconhecidos tais como o CIS *Benchmarks*, NIST ou recomendações do fornecedor. Deve-se garantir que soluções de software desenvolvidas internamente não alterem ou enfraqueçam essas configurações, e quaisquer exceções devem ser formalmente justificadas, aprovadas e documentadas. A conformidade com as configurações deverá ser verificada regularmente por auditorias ou ferramentas automatizadas.

Normas de referência: não identificada.

16.8	O órgão separa sistemas de produção e não produção?	GI2

Manter ambientes separados para sistemas de produção e não produção.

Normas de referência: não identificada.

16.9	O órgão treina desenvolvedores em conceitos de segurança de aplicações e codificação segura?	GI2

Treinar todos os responsáveis pelo desenvolvimento de software sobre escrever código seguro e sobre suas responsabilidades específicas. O treinamento deve incluir princípios gerais de segurança e práticas padrão de segurança para aplicações. Deve ser realizado pelo menos uma vez por ano e ser projetado de forma a promover a segurança dentro da equipe de desenvolvimento e criar uma cultura de segurança entre os desenvolvedores.

Normas de referência: NC nº 17/IN01/DSIC/GSIPR; NC nº 18/IN01/DSIC/GSIPR; Decreto nº 12.572/2025, art. 3º, IV, art. 4º, VI e art. 10, V.

16.10	O órgão aplica princípios de *design* seguro em arquiteturas de aplicações?	GI2

Aplicar princípios de *design* seguro em arquiteturas de aplicações. Os princípios de design seguro incluem o conceito de privilégio mínimo e a aplicação de mediação para validar cada operação que o usuário faz, promovendo o conceito de “nunca confiar nas entradas do usuário”. Os exemplos incluem garantir que a verificação explícita de erros seja realizada e documentada para todas as entradas, incluindo tamanho, tipo de dados e intervalos ou formatos aceitáveis. O design seguro também significa minimizar a superfície de ataque da infraestrutura da aplicação, como desligar portas e serviços desprotegidos, remover programas e arquivos desnecessários, renomear ou remover contas padrão, entre outros.

Normas de referência: não identificada.

16.11	O órgão reutiliza os módulos ou serviços validados quanto aos requisitos de segurança das aplicações?	GI2

Reutilizar módulos ou serviços validados quanto aos requisitos de segurança, como gestão de identidade, criptografia e auditoria de *logs*. O uso de recursos nativos de sistemas operacionais ou ambientes de desenvolvimento em funções críticas de segurança reduz a carga de trabalho dos desenvolvedores e minimiza a probabilidade de erros de design ou de implementação. Os sistemas operacionais modernos fornecem mecanismos eficazes para identificação, autenticação, autorização, criação e manutenção de logs de auditoria, disponibilizando tais mecanismos para as aplicações. Usar apenas algoritmos de criptografia padronizados, atualmente aceitos e amplamente revisados.

Normas de referência: não identificada.

16.12	O órgão implementa verificações de segurança em nível de código?	GI3

Utilizar ferramentas de análise estáticas e dinâmicas, *Static Application Security Testing* (SAST) e *Dynamic Application Security Testing* (DAST), dentro do ciclo de vida da aplicação para verificar se as práticas de codificação seguras estão sendo utilizadas na organização.

Normas de referência: não identificada.

16.13	O órgão realiza teste de intrusão de aplicação (*pentest*)?	GI3

Realizar testes de intrusão em aplicações. Para aplicações críticas, o teste de intrusão autenticado é mais adequado para localizar vulnerabilidades de codificação e de negócios do que a varredura de código e o teste de segurança automatizados. O teste de intrusão depende da habilidade do testador para manipular manualmente uma aplicação como um usuário autenticado e não autenticado.

Normas de referência: Decreto nº 12.573/2025, art. 4º, IV, art. 4º, IX.

16.14	O órgão realiza a modelagem de ameaças?	GI3

Realizar a modelagem de ameaças. A modelagem de ameaças é o processo de identificar e abordar as falhas de design de segurança da aplicação em um projeto, antes que o código seja criado. É conduzido por profissionais especialmente treinados que avaliam o design da aplicação e medem os riscos de segurança para cada ponto de entrada e nível de acesso. O objetivo é mapear a aplicação, a arquitetura e a infraestrutura de uma forma estruturada para entender todos os pontos fracos.

Normas de referência: não identificada.

5.17 CONTROLE 17: Gestão de incidentes

Visão geral

Estabelecer um programa para desenvolver e manter um processo de gestão de incidentes (por exemplo, políticas, planos, procedimentos, funções definidas, treinamento e comunicações) para preparar, detectar e responder rapidamente a um ataque.

Por que esse controle é crítico?

Um programa completo de segurança da informação deve incluir proteção, detecção, resposta e recuperação, mas organizações imaturas tendem a negligenciar as ações resposta e recuperação, limitando-se a restaurar sistemas sem compreender o incidente. O objetivo da resposta a incidentes é identificar ameaças, conter sua propagação e remediar antes que causem danos, evitando um ciclo constante de ataques.

Proteções não são 100% eficazes; sem um plano documentado, mesmo boas equipes terão dificuldades em conduzir investigações, reportar, coletar dados, gerenciar responsabilidades, seguir requisitos legais e comunicar-se adequadamente para entender, controlar e recuperar-se do incidente.

Além da detecção, contenção e erradicação, a comunicação com as partes interessadas é essencial. A liderança deve entender os impactos potenciais para priorizar decisões de remediação ou restauração baseadas em conformidade, acordos, receita ou missão.

O tempo entre o ataque e sua identificação pode durar dias, semanas ou meses. Quanto mais tempo o invasor permanecer, mais ele se integra e cria formas de manter acesso persistente. Esse tempo é crítico especialmente com *ransomwares*, que frequentemente combinam roubo de dados antes da criptografia para extorsão.

Procedimentos e ferramentas

Mesmo em organizações com recursos limitados para resposta a incidentes, é fundamental possuir um plano documentado, incluindo fontes de proteção e detecção, contatos para suporte e planos de comunicação para liderança, agentes públicos, reguladores, parceiros e demais usuários.

Após definir os procedimentos, a equipe de resposta deve realizar treinamentos periódicos baseados em cenários de ataque adaptados às ameaças e impactos potenciais da organização. Esses exercícios ajudam a equipe e a liderança a entender seus papéis, identificando lacunas e atualizando processos conforme necessário.

Organizações mais maduras devem incorporar inteligência de ameaças ou caça a ameaças no processo de resposta, permitindo uma postura proativa ao monitorar atacantes e suas táticas, melhorando a rapidez na detecção e remediação.

As ações deste controle fornecem passos prioritários importantes para fortalecer a segurança da informação e devem fazer parte de qualquer plano abrangente de resposta a incidentes. Além disso, recomenda-se os seguintes recursos dedicados a este tema:

- serviços, alertas e recomendações do Centro Integrado de Segurança Cibernética (CISC GOV.BR): https://www.gov.br/cisc/pt-br

- Guia de Resposta a Incidentes de Segurança Cibernética do *Council of Registered Security Testers* (CREST): o CREST fornece orientação, padrões e conhecimento sobre uma ampla variedade de tópicos de defesa cibernética - https://www.crest-approved.org/wp-content/uploads/2022/04/CSIR-Procurement-Guide-1.pdf

Lista de medidas

ID	Título, descrição e normas de referência	GI
17.1	**O órgão designou agente responsável, e respectivo substituo, para gerenciar a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR)?**	GI1
	Designar formalmente o agente responsável, e respectivo substituto, entre servidores públicos ocupantes de cargo efetivo ou militares de carreira da organização. Compete ao agente responsável chefiar e gerenciar a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR), além de criar os procedimentos internos, distribuir tarefas para a ETIR e ser a interface com o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov).	
	Normas de referência: IN GSI/PR nº 1/2020, art. 15, IV; NC n° 05/IN01/DSIC/GSIPR.	
17.2	**O órgão estabelece e mantém informações de contato para notificar incidentes de segurança da informação?**	GI1
	Estabelecer e manter informações de contato para as partes que precisam ser informadas sobre incidentes de segurança da informação, tais como equipe interna, provedores de serviço, unidade jurídica, provedores de seguro de cibersegurança, áreas de comunicação interna. A comunicação deve ocorrer entre a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) e, no mínimo, o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov) e o Centro Integrado de Segurança Cibernética do Governo Digital (CISC Gov.br). Verificar os contatos periodicamente para garantir que as informações estejam atualizadas.	
	Normas de referência: NC nº 21/IN01/DSIC/GSIPR, 8; NC n° 05/IN01/DSIC/GSIPR, 10.6.	
17.3	**O órgão estabelece e mantém um processo institucional para notificar incidentes de segurança da informação?**	GI1
	Estabelecer e manter um processo institucional para que os agentes públicos e demais pessoas possam notificar incidentes de segurança da informação. O processo deve incluir o prazo e o mecanismo para a comunicação, o pessoal a quem comunicar e as informações mínimas a serem comunicadas. É importante certificar-se de que o processo está publicamente disponível para todos os agentes públicos da organização. Deve ser realizada uma revisão periódica deste processo ou quando ocorrerem mudanças significativas na organização que possam impactar esta medida.	
	Normas de referência: NC nº 21/IN01/DSIC/GSIPR, Anexo A, 6.	

17.4	O órgão estabelece e mantém um processo de gestão de incidentes de segurança da informação?	GI2

Estabelecer e manter um processo de gestão de incidentes de segurança da informação que aborde as funções e responsabilidades, o plano de comunicação, o fluxo para o tratamento dos incidentes, o adequado registro das evidências e os requisitos de conformidade, considerando a NC nº 08/IN01/DSIC/GSIPR, a NC nº 21/IN01/DSIC/GSIPR e normas correlatas. Realizar a revisão deste processo de forma periódica ou quando ocorrerem mudanças significativas na organização que possam impactar esta medida.

Normas de referência: NC nº 08 /IN01/DSIC/GSIPR; NC nº 21/IN01/DSIC/GSIPR, 7 e 8; IN GSI/PR nº 1/2020, art. 19, X; *IN GSI/PR nº 5/2021, art. 13, IV, V e VI, art. 16, IV; Portaria GSI/PR nº 120/2022.

17.5	O órgão atribui funções e responsabilidades para gestão de incidentes de segurança da informação?	GI2

Atribuir as principais funções e responsabilidades para a gestão de incidentes de segurança da informação, incluindo equipe jurídica, TI, segurança da informação, instalações, relações públicas, recursos humanos, equipe de tratamento de incidentes e de analistas. Realizar a revisão deste processo de forma periódica ou quando ocorrerem mudanças significativas na organização que possam impactar esta medida.

Normas de referência: NC nº 21/IN01/DSIC/GSIPR, 8 ; IN GSI/PR nº 1/2020, art. 19, VI, IX.

17.6	O órgão define mecanismos de comunicação a ser realizado durante o tratamento de incidentes de segurança da informação?	GI2

Determinar quais mecanismos primários e secundários serão usados para notificar um incidente de segurança da informação e para se comunicar durante um incidente. Os mecanismos podem incluir ligações, mensagens, *chats*, *e-mails*, cartas, entre outros. Atentar ao fato de que certos mecanismos, como *e-mails*, podem ser afetados durante um incidente de segurança. Realizar a revisão desta medida de forma periódica ou quando ocorrerem mudanças significativas na organização que possam impactar esta medida.

Normas de referência: NC nº 08 /IN01/DSIC/GSIPR.

17.7	O órgão conduz exercícios de tratamento de incidentes de segurança da informação regularmente?	GI2

Planejar e conduzir exercícios e cenários rotineiros de tratamento de incidentes de segurança da informação para a equipe envolvida, de forma a manter a conscientização e a tranquilidade no caso de resposta a ameaças reais. Os exercícios devem testar os canais de comunicação, tomada de decisão e recursos técnicos da equipe de resposta a incidentes, contemplando a utilização das ferramentas e dados disponíveis. Realizar o exercício semestralmente ou em intervalos menores.

Normas de referência: não identificada.

17.8	O órgão realiza análises pós-incidente de segurança da informação?	GI2

Realizar análises pós-incidente de segurança da informação. As análises pós-incidente ajudam a prevenir a recorrência do incidente por meio da identificação de lições aprendidas e ações de acompanhamento.

Normas de referência: não identificada.

17.9	O órgão estabelece a diferença entre evento e incidente de segurança da informação?	GI3

Estabelecer e manter critérios para a diferenciação entre evento e incidente de segurança da informação. Os exemplos podem incluir: atividade anormal, vulnerabilidade de segurança, ameaça de segurança, violação de dados, incidente de privacidade. Realizar a revisão desta medida de forma periódica ou quando ocorrerem mudanças significativas na organização que possam impactar esta medida.

Normas de referência: não identificada.

* A IN GSI/PR nº 5/2021 estabelece os requisitos mínimos de segurança da informação para que órgãos e entidades da administração pública federal utilizem soluções de computação em nuvem, sendo uma norma de referência apenas para estes ambientes computacionais.

5.18 CONTROLE 18: Testes de intrusão

Visão geral

Testar a eficácia e a resiliência dos ativos institucionais e das soluções de *software*, identificando e explorando vulnerabilidades e simulando os objetivos e ações de um invasor.

Por que esse controle é crítico?

Uma postura defensiva eficaz requer um programa abrangente com políticas, governança, defesas técnicas robustas e ações adequadas das pessoas. Em ambientes complexos e dinâmicos, empresas devem testar periodicamente seus controles para identificar falhas e avaliar resiliência, compreendendo testes em redes, soluções de *software*, dispositivos, engenharia social em usuários e controle de acesso físico.

Testes de penetração são realizados para demonstrar um ataque e respectivas vulnerabilidades, verificar a operação das defesas ou validar a implementação correta delas. Testes de penetração independentes podem fornecer percepções valiosas sobre vulnerabilidades em ativos institucionais e soluções de *software*, incluindo falhas em processos e treinamentos, além de avaliar a eficácia dos controles, e fazer parte de um programa contínuo de segurança.

Diferentemente dos testes de vulnerabilidade (controle 7), que focam em identificar pontos fracos conhecidos sem explorar a profundidade do ataque, os testes de penetração envolvem exploração ativa para avaliar o impacto real. Análise de vulnerabilidade é geralmente

automatizada; testes de penetração exigem análise humana e uso de ferramentas específicas, algumas vezes envolvendo uso de ferramentas ou scripts personalizados.

Procedimentos e ferramentas

O teste de penetração inicia-se com o reconhecimento da organização e do ambiente, seguido pela varredura para identificação de vulnerabilidades em todos os ativos em escopo, evitando listas estáticas desatualizadas. Explorações são realizadas para demonstrar como um adversário pode comprometer a segurança ou alcançar objetivos maliciosos, abrangendo controles físicos, redes, soluções de *software* e engenharia social.

Testes de penetração são complexos, caros e apresentam riscos, devendo ser conduzidos por profissionais experientes. Podem causar falhas nos sistemas que vão desde possíveis instabilidades, englobando seu eventual desligamento, e até mesmo corromper dados. Destaca-se que os relatórios gerados precisam ser protegidos para evitar que forneçam instruções aos atacantes.

Cada organização deve definir um escopo claro e regras de engajamento, focando em ativos com informações valiosas e processos críticos, incluindo possíveis soluções de *software* de menor valor que possam ser usados para movimentos laterais. Regras devem contemplar horários, duração e abordagem, com poucos informados sobre o teste e um responsável designado para incidentes.

As medidas deste controle indicam passos prioritários para aprimorar a segurança. Além disso, recomenda-se o uso de alguns dos excelentes recursos abrangentes dedicados a este tema para apoiar a realização de testes de intrusão, além do planejamento, a gestão e a elaboração de relatórios de testes de segurança:

- testes de intrusão do Centro Integrado de Segurança Cibernética (CISC GOV.BR): https://www.gov.br/cisc/pt-br
- Metodologias de Teste de Intrusão da OWASP: https://owasp.org/www-project-web-security-testing-guide/latest/3-The_OWASP_Testing_Framework/1-Penetration_Testing_Methodologies
- Conselho de Normas de Segurança da Indústria de Meios de Pagamento (*Payment Card Industry Security Standards Council – PCI SSC*) – Guia de Testes de Intrusão: https://www.pcisecuritystandards.org/documents/Penetration-Testing-Guidance-v1_1.pdf

Lista de medidas

ID	Título, descrição e normas de referência	GI
18.1	**O órgão elabora e mantém um programa de teste de intrusão (*pentest*)?**	**GI2**
Estabelecer e manter um programa para testes de intrusão adequado ao tamanho, à complexidade e à maturidade da organização. O programa de teste de intrusão deve levar		

em consideração: o escopo do teste, como rede, aplicação web, *Application Programming Interface* (API), controles de instalações físicas; frequência; limitações, como horários aceitáveis e tipos de ataque excluídos; informações de contato; remediações, tais como o encaminhamento das descobertas internamente; e lições aprendidas.

Normas de referência: Decreto nº 12.573/2025, art. 4º, IX.

18.2	O órgão realiza testes de intrusão externos periódicos (*pentest*)?	GI2

Realizar testes de intrusão externos regularmente. O teste de intrusão externo deve ser reconhecido pela organização e deve ser capaz de detectar informações exploráveis que possam impactar a segurança dos ativos institucionais e soluções de software. Tal teste deve ser realizado por profissionais qualificados.

Normas de referência: não identificada.

18.3	O órgão corrige os resultados dos testes de intrusão (*pentest*)?	GI2

Corrigir as descobertas dos testes de intrusão com base no processo de correção de vulnerabilidade da organização. Isso deve incluir a determinação de um cronograma e nível de esforço com base no impacto e na priorização de cada descoberta identificada.

Normas de referência: não identificada.

18.4	O órgão valida as medidas de segurança?	GI3

Validar as medidas de segurança após cada teste de intrusão. Se necessário, modificar os conjuntos de regras e recursos para detectar as técnicas usadas durante o teste.

Normas de referência: não identificada.

18.5	O órgão realiza testes de intrusão internos periódicos (*pentest*)?	GI3

Realizar testes de intrusão internos periódicos com base nos requisitos do programa estabelecido pela medida 18.1. Realize o teste anualmente ou em intervalos menores.

Normas de referência: não identificada.

6 Controles do segmento de privacidade

Os controles e medidas de privacidade propostos no *framework* do PPSI 2.0 foram embasados especialmente na Lei Geral de Proteção de Dados Pessoais (LGPD), bem como nas seguintes resoluções vigentes emitidas pela ANPD até a data de publicação deste guia[3]:

- Resolução CD/ANPD nº 15, de 24 de abril de 2024 - Aprova o Regulamento de Comunicação de Incidente de Segurança [11].
- Resolução CD/ANPD nº 18, de 16 de julho de 2024 - Aprova o Regulamento sobre a atuação do encarregado pelo tratamento de dados pessoais [12].
- Resolução CD/ANPD nº 19, de 23 de agosto de 2024 - Aprova o Regulamento de Transferência Internacional de Dados e o conteúdo das cláusulas-padrão contratuais [13].

Diferentemente das medidas de segurança da informação, as quais seguem o modelo de boas práticas do CIS e foram correlacionadas no *framework* do PPSI 2.0 à legislação brasileira aplicável, as medidas propostas para privacidade são primordialmente consideradas obrigações legais à luz da LGPD e resoluções mencionadas.

Este conjunto de controles e respectivas medidas foram elaborados objetivando elevar o nível de conformidade à LGPD pelos órgãos e entidades do SISP, consequentemente aprimorando o grau de maturidade em privacidade e proteção de dados pessoais.

Destaca-se também que, tendo em vista o papel fundamental da ANPD na orientação e normatização da proteção de dados pessoais, a Agência vem elaborando guias orientativos[4] com o objetivo de delinear parâmetros que possam auxiliar órgãos e entidades nas atividades de conformidade à LGPD. As orientações apresentadas no Guia Orientativo de Tratamento de Dados Pessoais pelo Poder Público constituem um primeiro passo no processo de delimitação das interpretações sobre a LGPD aplicáveis ao Poder Público [14].

As medidas de privacidade propostas no *framework* do PPSI 2.0 foram agrupadas em sete controles:

- registro das operações de tratamento de dados pessoais;
- ações de prevenção;
- encarregado e direitos dos titulares;
- contratos, acordos e instrumentos congêneres;
- análise das operações de tratamento;
- compartilhamento e transferência internacional;
- princípios da LGPD;

[3] Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd

[4] Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/materiais-educativos

Cada controle e respectivo conjunto de medidas estão associados a práticas concretas que devem ser avaliadas e implementadas pelas organizações. As medidas incluem desde o registro do ciclo de vida dos dados, análise deste registro para possíveis adequações, até cláusulas contratuais, elaboração de Relatórios de Impacto à Proteção de Dados Pessoais (RIPDs) e medidas de anonimização.

A seguir, são apresentados os controles de privacidade, incluindo a visão geral, importância do controle, procedimentos e ferramentas para sua implementação, e a lista de medidas relacionadas.

6.1 CONTROLE 19: Registro das operações de tratamento de dados pessoais

Visão geral

Este controle estabelece a necessidade de a organização elaborar e manter, de forma contínua, o registro das operações de tratamento de dados pessoais, independentemente do meio utilizado (físico ou digital). O registro deve descrever detalhadamente o fluxo dos dados pessoais, desde a coleta até o descarte, contemplando informações como as fontes, finalidades, hipóteses legais que amparam o tratamento, tempo de retenção, soluções tecnológicas utilizadas, agentes de tratamento envolvidos, compartilhamentos, transferências internacionais.

Por que esse controle é crítico?

O registro das operações de tratamento de dados pessoais constitui uma exigência legal expressa no artigo 37 da LGPD, sendo considerado o ponto de partida para a governança, auditoria e avaliações de conformidade dos tratamentos realizados pelo órgão.

Na ausência de registros formais, completos e atualizados, a organização perde a capacidade de demonstrar conformidade, identificar riscos específicos vinculados aos processos e fluxos de dados pessoais, e atender às solicitações de titulares ou de autoridades fiscalizadoras. Ademais, o registro sistemático viabiliza avaliações de risco, suporta a elaboração de avisos de privacidade, RIPDs e permite a correção tempestiva de tratamentos em desconformidade à LGPD.

Procedimentos e ferramentas

Para a efetiva implementação deste controle, recomenda-se a instituição de processo formal, documentado e continuamente revisado para o registro e atualização das operações de tratamento de dados pessoais, com papéis definidos (por exemplo, responsável pelo registro e revisor) e periodicidade mínima de revisão.

Recomenda-se a adoção de repositório centralizado que possibilite funcionalidades de busca, versionamento e geração de relatórios. Ademais, é recomendada a padronização dos modelos para registro, abarcando informações essenciais como finalidades, bases legais, tipos e

categorias de dados pessoais e dados pessoais sensíveis, fluxos de tratamento e demais elementos necessários ao atendimento das exigências legais e às necessidades institucionais.

Lista de medidas

ID	Título, descrição e normas de referência
19.1	**O órgão elabora e mantém processo para registrar as operações de tratamento de dados pessoais?**
Estabelecer e manter processo documentado para registro das operações de tratamento de dados pessoais, independentemente do meio em que os dados pessoais são tratados, a ser amplamente divulgado na organização, que contemple o conteúdo disposto nas medidas 19.1 a 19.4 e estabeleça a periodicidade da atualização dos registros.	
Normas de referência: Lei nº 13.709/2018, art. 37; Resolução CD/ANPD nº 15/2024, art. 8º.	
19.2	**O órgão inclui no registro das operações de tratamento a descrição do fluxo dos dados pessoais?**
Assegurar que o registro das operações de tratamento de dados pessoais contemple a descrição dos fluxos dos dados pessoais, a fonte (origem), as finalidades e hipóteses do tratamento (e respectiva previsão legal, quando aplicável), os tempos de retenção, as soluções de software que viabilizam o tratamento dos dados pessoais. A descrição do fluxo de dados pessoais deve contemplar desde a coleta até o descarte, passando por todas as etapas de uso dos dados pessoais. Atentar para o adequado registro das características dos tratamentos de dados pessoais sensíveis.	
Normas de referência: Lei nº 13.709/2018, art. 37; Resolução CD/ANPD nº 15/2024, art. 8º.	
19.3	**O órgão inclui no registro das operações de tratamento de dados pessoais os agentes, os compartilhamentos, as transferências internacionais e as abrangências geográficas do tratamento?**
Assegurar que o registro das operações de tratamento de dados pessoais contemple, além do indicado nas medidas 19.2 e 19.4: os agentes de tratamento (controladores, singulares ou conjuntos, e operadores), os contratos, acordos ou instrumentos congêneres firmados com os agentes de tratamento e as abrangências geográficas do tratamento. Incluir os compartilhamentos de dados pessoais com terceiros e as transferências internacionais (com respectivos tipos de dados pessoais, finalidades e hipóteses de tratamento, além de países ou organismos internacionais para os quais os dados pessoais são transferidos).	
Normas de referência: Lei nº 13.709/2018, art. 37; Resolução CD/ANPD nº 15/2024, art. 8º.	
19.4	**O órgão inclui no registro das operações de tratamento de dados pessoais os tipos de dados tratados e as categorias de titulares?**
Assegurar que o registro das operações de tratamento de dados pessoais contemple, além do indicado nas medidas 19.2 e 19.3: os tipos de dados pessoais tratados, sua natureza (se	

sensíveis ou não) e respectiva classificação (cadastrais, financeiros, acadêmicos, dados de saúde, biométricos, entre outros); as categorias de titulares de dados pessoais (clientes, funcionários, agentes públicos, estudantes, fornecedores, entre outros). Incluir indicação sobre tratamento de dados pessoais de vulneráveis, a exemplo de crianças, adolescentes e idosos.

Normas de referência: Lei nº 13.709/2018, art. 37; Resolução CD/ANPD nº 15/2024, art. 8º.

6.2 CONTROLE 20: Ações de prevenção

Visão geral

Este controle compreende um conjunto de medidas administrativas voltadas à mitigação de riscos relacionados ao tratamento de dados pessoais, visando reduzir a probabilidade de violações de privacidade. Abrange, entre outros aspectos, a gestão de incidentes com dados pessoais, a incorporação do princípio da privacidade desde a concepção (*privacy by design*) e o fortalecimento da cultura organizacional em privacidade e proteção de dados pessoais por meio de ações de conscientização e capacitação contínuas.

Por que esse controle é crítico?

A implementação de medidas preventivas reduz a necessidade de adoção de ações corretivas posteriores, diminui custos operacionais e reforça a confiança de titulares e terceiros em relação ao tratamento de dados pessoais conduzido pela organização. Ademais, essas medidas são exigidas por orientações e resoluções emanadas pela ANPD, compondo requisito fundamental de conformidade. Destaca-se a relevância das iniciativas de conscientização, que possibilitam o entendimento e a aplicação de práticas seguras por todos os agentes públicos, mitigando, de forma proativa, riscos de incidentes como vazamentos de dados e ataques cibernéticos.

Procedimentos e ferramentas

A efetividade deste controle pressupõe a instituição de processos formais e sistematizados que integrem o requisito de privacidade em todas as iniciativas da organização – abrangendo projetos, contratações, novos processos, entre outros.

Para concretizar a conformidade à LGPD e efetivar a proteção dos dados pessoais sob a responsabilidade da organização, recomenda-se o desenvolvimento contínuo da conscientização dos agentes públicos, por meio de ações periódicas, campanhas informativas, plataformas educacionais, webinários, materiais de divulgação temática e *quizzes* interativos. O programa de conscientização em proteção de dados pessoais pode estar associado ao programa de conscientização em segurança da informação estabelecido pelo controle 14. Medidas voltadas à avaliação periódica do conhecimento dos agentes públicos e à integração de conteúdos de proteção de dados pessoais nos programas de formação inicial e continuada são fundamentais. É igualmente recomendada a disponibilização de canais internos para

contato com o Encarregado pelo tratamento de dados pessoais (medida 21.5) para prestar esclarecimentos e orientações relacionadas à LGPD e às práticas seguras.

Por fim, sugere-se a elaboração de programas de capacitação específicos, adequados ao perfil e às atribuições de cada agente público, especialmente considerando a sua atuação nas ações de conformidade, e assegurando a atualização constante dos conteúdos e a aderência dos treinamentos à legislação e às resoluções da ANPD vigentes.

Para uma abordagem mais abrangente deste tópico, considerar os seguintes recursos:

- materiais educativos disponibilizados pelo Centro de Excelência em Privacidade e Segurança (CEPS GOV.BR): https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/centro-de-excelencia-em-privacidade-e-seguranca
- NIST® SP 800-50 - Construindo um Programa de Aprendizagem em Segurança Cibernética e Privacidade: https://csrc.nist.gov/pubs/sp/800/50/r1/final

Lista de medidas

ID	Título, descrição e normas de referência
20.1	**O órgão implementa processo de gestão de incidentes com dados pessoais?**
Estabelecer, manter e implementar um processo documentado de gestão de incidentes com dados pessoais, contemplando ações para o tratamento dos incidentes, incluindo plano de resposta a incidentes e remediação, nos termos da Lei nº 13.709/2018 e da Resolução CD/ANPD nº 15/2024, que aborde funções e responsabilidades, principalmente acerca do registro do incidente e sobre a eventual comunicação do incidente à ANPD e aos titulares de dados pessoais. Realizar a revisão deste processo de forma periódica ou quando ocorrerem mudanças significativas na organização que possam impactar esta medida. Este processo pode ser incorporado ao gerenciamento de resposta a incidentes de segurança da informação disposto no Controle 17 do PPSI.	
Normas de referência: Lei nº 13.709/2018, arts. 48 e 50, § 2º, I, g; Resolução CD/ANPD nº 15/2024.	
20.2	**O órgão implementa programa de conscientização em privacidade e proteção de dados pessoais?**
Estabelecer e manter um programa de conscientização em privacidade e proteção de dados pessoais, com os objetivos de promover tal cultura na organização, sensibilizar seus agentes públicos sobre responsabilidades e procedimentos relacionados ao tema e sobre como tratar os dados pessoais de forma segura. Revisar e atualizar o conteúdo periodicamente ou quando ocorrerem mudanças significativas na organização que possam impactar esta medida, em especial como uma das medidas de resposta a incidentes com dados pessoais.	
Normas de referência: Lei nº 13.709/2018, arts 6º, VII e VIII, e arts. 46, 47 e 50.	

20.3	O órgão implementa ações para capacitação sobre privacidade e proteção de dados pessoais?

Incluir nos instrumentos de desenvolvimento de pessoas da organização, a exemplo do Plano de Desenvolvimento de Pessoas, as necessidades de desenvolvimento em privacidade e proteção de dados pessoais para agentes públicos que atuem em funções específicas, de modo a atender suas competências específicas, e promover a execução de tais instrumentos. Exemplos de necessidades de desenvolvimento incluem cursos de adequação de contratos e instrumentos congêneres à Lei nº 13.709/2018 e elaboração de RIPDs.

Normas de referência: Lei nº 13.709/2018, arts 6º, VII e VIII, e arts. 46, 47 e 50; Decreto nº 12.572/2025, art. 3º, IV, art. 4º, VI e art. 10, V.

20.4	O órgão possui um processo para promover a privacidade desde a fase de concepção do produto ou do serviço até a sua execução?

Estabelecer e manter um processo objetivando a privacidade desde a fase de concepção do produto ou do serviço até a sua execução (*privacy by design*), contemplando o desenvolvimento de novas iniciativas, ações, projetos ou programas que envolvam novas operações de tratamento de dados pessoais. O processo deve promover a implementação de medidas de segurança, técnicas e administrativas, incluindo as estabelecidas no PPSI.

Normas de referência: Lei nº 13.709/2018, art. 46, § 2º.

6.3 CONTROLE 21: Encarregado e direitos dos titulares

Visão geral

Este controle tem por objetivo estabelecer medidas que assegurem condições adequadas para a atuação do Encarregado pelo tratamento de dados pessoais, bem como aperfeiçoar demais mecanismos organizacionais para assegurar o exercício efetivo dos direitos dos titulares. Inclui-se, nesse âmbito, a implementação de canais de atendimento acessíveis e o desenvolvimento de processos claros para tratamento de solicitações, os quais devem ser integrados aos fluxos de diferentes áreas, como tecnologia da informação, segurança da informação e jurídico.

Por que esse controle é crítico?

A atuação do Encarregado e a disponibilidade de canais efetivos de atendimento aos titulares são requisitos fundamentais para o cumprimento das obrigações previstas na LGPD e na Resolução CD/ANPD nº 18/2024. Processos bem estruturados e executados possibilitam o atendimento tempestivo dos direitos dos titulares, fortalecendo a confiança na organização e promovendo a transparência e a responsabilização e prestação de contas. A ausência de mecanismos adequados de resposta compromete o relacionamento com os titulares e pode ensejar riscos reputacionais e legais para a organização.

Procedimentos e ferramentas

Para a implementação deste controle, recomenda-se:

- criar, divulgar e manter canais de atendimento acessíveis, tais como portais eletrônicos, formulários digitais ou centrais de atendimento dedicadas, com mecanismos de autenticação que assegurem a identificação do titular;
- definir fluxos de atendimento alinhados aos prazos legais e às melhores práticas, mantendo modelos padronizados de resposta, critérios de triagem e procedimentos de escalonamento das solicitações, conforme as áreas envolvidas (negócio, TI, jurídico, ouvidoria);
- assegurar a documentação e rastreabilidade das solicitações – utilizando, por exemplo, sistemas de *ticketing* integrados aos registros das operações de tratamento de dados pessoais (controle 19) – e desenvolver relatórios de desempenho;
- estabelecer mecanismos de auditoria e avaliação contínua dos canais e processos, garantindo transparência, prestação de contas e aderência aos requisitos legais.

Considerar o seguinte material como referência para implementação das medidas previstas neste controle:

- ANPD – Guia Orientativo - Atuação do encarregado pelo tratamento de dados pessoais: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia_da_atuacao_do_encarregado_anpd.pdf/view

Lista de medidas

ID	Título, descrição e normas de referência
21.1	**O órgão provê os meios necessários para que o encarregado exerça suas atividades e atribuições?**
Disponibilizar ao encarregado pelo tratamento de dados pessoais os recursos necessários – entre eles humanos, técnicos e administrativos –, para que preste assistência e orientação à organização com autonomia técnica e evitando situações que possam configurar conflito de interesse. Garantir ao encarregado o acesso direto aos responsáveis, inclusive de maior nível hierárquico, pela tomada de decisões estratégicas sobre o tratamento de dados pessoais. Observar o disposto no art. 41 da Lei nº 13.709/2018, na Resolução CD/ANPD nº 18/2024 e no art. 3º da IN SGD/ME nº 117/2020.	
Normas de referência: Lei nº 13.709/2018, art. 41; Resolução CD/ANPD nº 18/2024, art. 10.	
21.2	**O órgão disponibiliza meios céleres, eficazes e adequados para viabilizar a comunicação dos titulares com o encarregado e o exercício de direitos?**
Disponibilizar solução para que os titulares de dados pessoais, por meios céleres, eficazes e adequados, possam realizar solicitações e reclamações ao encarregado e receber as respectivas respostas.	

Normas de referência: Lei nº 13.709/2018, Capítulo III e art. 41; Resolução CD/ANPD nº 18/2024, art. 10, I.

21.3 O órgão possui processo para atendimento aos direitos dos titulares de dados pessoais?

Estabelecer um processo documentado para atendimento de requisição do titular de dados pessoais ou de seu representante legalmente constituído. Recomenda-se que o processo inclua a identificação dos papéis e responsabilidades das unidades da organização quanto às medidas necessárias para o atendimento da solicitação, considerando principalmente as atribuições do encarregado pelo tratamento de dados pessoais dispostas na Lei nº 13.709/2018 e na Resolução CD/ANPD nº 18/2024, e inclua prazos e requisitos para o fornecimento das informações pertinentes e eventuais interações entre o encarregado e as unidades objetivando atendimento dos direitos do titular. Sugere-se consignar no processo que o requerimento será atendido sem custos para o titular e, a seu critério, as informações e dados serão fornecidos por meio eletrônico, seguro e idôneo, ou sob forma impressa. A organização deve ainda atentar para que o processo considere que os dados pessoais referentes ao exercício regular de direitos não podem ser utilizados em prejuízo do titular.

Normas de referência: Lei nº 13.709/2018, Capítulo III e arts. 23, 41, 48 e 50; Resolução CD/ANPD nº 18/2024, art. 10, IV.

21.4 O órgão divulga publicamente e mantém atualizadas a identidade e as informações de contato do encarregado e de seu substituto?

Divulgar publicamente e manter atualizados, no mínimo, o nome completo e as informações de contato do encarregado pelo tratamento de dados pessoais e de seu substituto – em local de destaque e de fácil acesso no sítio eletrônico, de forma clara e objetiva –, viabilizando também o exercício de direitos pelos titulares e o recebimento de comunicações da ANPD.

Normas de referência: Lei nº 13.709/2018, art. 41; Resolução CD/ANPD nº 18/2024, arts. 8º e 9º.

21.5 O órgão solicita assistência e orientação do encarregado quando realiza atividades e toma decisões estratégicas referentes ao tratamento de dados pessoais?

Solicitar assistência e orientação do encarregado quando realizar atividades e tomar decisões estratégicas referentes ao tratamento de dados pessoais. Exemplos de implementações desta medida incluem: elaborar e divulgar procedimento e tecnologia para registro das solicitações ao encarregado; divulgar internamente o canal de contato com o encarregado e sua atribuição quanto ao fornecimento de orientações ao controlador.

Normas de referência: Lei nº 13.709/2018, art. 41; Resolução CD/ANPD nº 18/2024, arts. 10, II, e 16.

21.6 O órgão possui processo para revisar, a pedido do titular, decisões tomadas com base em tratamento automatizado de dados pessoais?

Estabelecer um processo documentado para revisar, a pedido do titular ou do seu representante legal, as decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem os interesses do titular, inclusive aquelas decisões que definam seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. O processo deve prever o fornecimento, quando solicitado, de informações claras e adequadas acerca dos critérios e procedimentos utilizados para a tomada de decisões automatizadas pela organização.

Normas de referência: Lei nº 13.709/2018, art. 20.

6.4 CONTROLE 22: Contratos, acordos e instrumentos congêneres

Visão geral

Este controle visa assegurar a incorporação de cláusulas contratuais, requisitos e práticas eficazes que garantam a proteção dos dados pessoais nas relações mantidas com terceiros, tais como fornecedores, parceiros, prestadores de serviço, convênios e demais agentes de tratamento. Abrange a diligência pré-contratual para avaliação da conformidade e capacidade técnica dos agentes, a inclusão de cláusulas mínimas obrigatórias relativas à proteção de dados pessoais e procedimentos para o acompanhamento do cumprimento contratual.

Por que esse controle é crítico?

Grande parte dos incidentes envolvendo dados pessoais decorre de falhas ou condutas inadequadas de terceiros contratados pela organização. Contratos mal elaborados ou a ausência de mecanismos eficazes de fiscalização aumentam significativamente a exposição legal, operacional e reputacional do órgão. A adoção de cláusulas padronizadas, alinhadas à LGPD e à Resolução CD/ANPD nº 19/2024, contribui para reduzir os riscos, assegurar a responsabilização adequada dos agentes no tratamento e facilitar a resposta eficaz a incidentes, especialmente em casos de vazamento ou uso indevido por terceiros.

Procedimentos e ferramentas

Para a implementação efetiva deste controle, recomenda-se:

- instituir processos que avaliem a capacidade técnica, organizacional e de conformidade dos agentes de tratamento antes da formalização contratual;
- incluir cláusulas contratuais essenciais que detalhem os objetivos do tratamento, obrigações de segurança da informação, eventuais restrições à subcontratação, procedimentos para reporte e gestão de incidentes, medidas administrativas e técnicas para proteção dos dados pessoais, regras concernentes à transferência internacional, responsabilidades em relação a demandas dos titulares e cláusulas de encerramento, devolução ou destruição segura dos dados pessoais;

- manter um repositório e estabelecer revisões periódicas de contratos, convênios e instrumentos congêneres, acompanhadas de auditorias ou relatórios padronizados para verificar o cumprimento das obrigações relativas à proteção de dados pessoais;
- padronizar procedimentos de encerramento contratual que assegurem a anonimização, devolução ou descarte seguro dos dados pessoais tratados, acompanhados de comprovação documental.

Lista de medidas

ID	Título, descrição e normas de referência
22.1	**O órgão estabelece em contrato, convênio ou instrumento congênere os papéis e responsabilidades dos agentes de tratamento envolvidos?**
Estabelecer e manter contratos, convênios e instrumentos congêneres com agentes de tratamento de dados pessoais. Nas situações em que a organização realiza compartilhamento restrito e específico de dados pessoais, formalizá-lo por meio do documento de interoperabilidade, disposto no Decreto nº 10.046/2019. Recomenda-se que referidos documentos contenham os papéis e responsabilidades dos agentes envolvidos, além de cláusulas que objetivem garantir a adoção de medidas técnicas (ex.: criptografia, controle de acesso, pseudonimização e testes de intrusão) e administrativas (ex.: termos de responsabilidade, acordos de confidencialidade e termos de sigilo) adequadas para o cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados pessoais previstos na Lei nº 13.709/2018, incluindo as resoluções da ANPD aplicáveis, a exemplo da adoção das cláusulas-padrão contratuais estabelecidas na Resolução CD/ANPD nº 19/2024 para as operações de tratamento que envolvam transferência internacional de dados pessoais.	
Normas de referência: Lei nº 13.709/2018, arts. 16, 33, 39, 42, 46, 47, 49, 50 e 52; Resolução CD/ANPD nº 19/2024, Anexo, arts. 2º, 17 e 27; IN SGD/ME nº 94/2022; Portarias SGD/MGI nº 5.950/2023, nº 750/2023, nº 6.679/2024, nº 1.070/2023, nº 6.680/2024, nº 2.715/2023 e nº 370/2023.	
22.2	**O órgão avalia se os agentes de tratamento aplicam medidas aptas a proteger os dados pessoais?**
Avaliar se os agentes de tratamento aplicam as medidas técnicas e administrativas estabelecidas em contrato, convênio ou instrumento congênere. O escopo da avaliação pode variar de acordo com a complexidade do tratamento de dados pessoais e os riscos no tratamento (tratamento de dados pessoais sensíveis; ocorrência de transferência internacional de dados pessoais, considerando o Capítulo V da Lei nº 13.709/2018 e a Resolução CD/ANPD nº 19/2024; tratamento de dados pessoais de crianças, adolescentes ou idosos; entre outros), podendo ser realizado por meio da análise de relatórios de avaliação padronizados e aplicação de questionários. A avaliação dos agentes de tratamento	

deve ser realizada de forma periódica e na medida que contratos, acordos de cooperação ou instrumentos congêneres forem firmados ou atualizados.

Normas de referência: Lei nº 13.709/2018, arts. 16, 33, 39, 42, 46, 47, 49, 50 e 52; Resolução CD/ANPD nº 19/2024, Anexo, arts. 2º, 17 e 27; IN SGD/ME nº 94/2022; Portarias SGD/MGI nº 5.950/2023, nº 750/2023, nº 6.679/2024, nº 1.070/2023, nº 6.680/2024, nº 2.715/2023 e nº 370/2023.

22.3	**O órgão encerra de forma segura o contrato, acordo ou instrumento congênere com os agentes de tratamento de dados pessoais?**

Realizar de forma segura o encerramento de contrato, acordo ou instrumento congênere, considerando inclusive o disposto na Resolução CD/ANPD nº 19/2024. Algumas ações que podem ser utilizadas para realizar este encerramento são: solicitar anonimização, devolução ou descarte com segurança dos dados pessoais tratados; encerrar o fluxo de dados pessoais.

Normas de referência: Lei nº 13.709/2018, arts. 15, 16, 39, 42, 46, 47, 49, 50; Resolução CD/ANPD nº 19/2024, Anexo, arts. 2º, 17 e 27; IN SGD/ME nº 94/2022; Portaria SGD/MGI nº 5.950/2023.

22.4	**O órgão incluiu cláusulas protetivas de dados pessoais nos contratos, acordos de cooperação e instrumentos congêneres vigentes em que há tratamento de dados pessoais?**

Revisar e adaptar os contratos, acordos de cooperação e instrumentos congêneres vigentes em que há tratamento de dados pessoais, de modo a adequá-los à Lei nº 13.709/2018 e a normas correlatas, considerando também as medidas deste Controle 22 e a Resolução CD/ANPD nº 19/2024.

Normas de referência: Lei nº 13.709/2018, arts. 16, 33, 39, 42, 46, 47, 49, 50 e 52; Resolução CD/ANPD nº 19/2024, Anexo, arts. 2º, 17 e 27; IN SGD/ME nº 94/2022; Portarias SGD/MGI nº 5.950/2023, nº 750/2023, nº 6.679/2024, nº 1.070/2023, nº 6.680/2024, nº 2.715/2023 e nº 370/2023.

6.5 CONTROLE 23: Análise das operações de tratamento

Visão geral

Este controle consolida práticas sistemáticas de análise de cada operação de tratamento de dados pessoais registrada no controle 19, promovendo a avaliação e aplicação de medidas de conformidade específicas sobre as operações de tratamento. Inclui-se, entre as medidas previstas, a revisão criteriosa das finalidades declaradas para o tratamento, a aderência às hipóteses legais aplicáveis, assim como a elaboração de Relatórios de Impacto à Proteção de Dados Pessoais (RIPD) quando aplicável.

Por que esse controle é crítico?

A adoção de análises estruturadas possibilita a identificação precoce de riscos potenciais à privacidade e aos direitos dos titulares, o que viabiliza a adoção tempestiva de medidas compensatórias ou mitigadoras. Os RIPDs e as avaliações formais correspondentes são exigências frequentes das melhores práticas internacionais e das diretrizes da ANPD, especialmente em cenários de alto risco, tais como o tratamento de dados pessoais sensíveis, o uso de novas tecnologias ou práticas de perfilagem. Tais instrumentos também fortalecem a demonstração de responsabilização e a prestação de contas por parte dos agentes de tratamento.

Procedimentos e ferramentas

Recomenda-se a definição clara de critérios para análise das operações de tratamento, incluindo a eventual necessidade de elaboração de RIPD, ponderando sobre fatores como tratamento de dados sensíveis, volumes expressivos de dados pessoais, decisões automatizadas e transferências internacionais de dados. Deve-se estabelecer modelos padronizados para o RIPD e designar equipe multidisciplinar responsável pela avaliação, envolvendo o encarregado pelo tratamento de dados pessoais e as áreas de privacidade, jurídica, segurança da informação e negócios.

Os resultados das análises podem ser integrados ao processo de registro estabelecido no controle 19, bem como incorporados ao planejamento e implementação das medidas de mitigação de riscos. Ferramentas de apoio podem abranger *checklists*, sistemas de gestão de riscos e fluxos de trabalho que assegurem rastreabilidade das decisões, armazenamento de evidências e revisões documentadas.

Para a implementação deste controle, recomenda-se o estudo dos seguintes guias orientativos produzidos pela ANPD:

- Guia Orientativo – Tratamento de dados pessoais pelo Poder Público: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia_orientativo_tratamento_de_dados_pessoais_pelo_poder_publico
- Guia Orientativo – Hipóteses legais de tratamento de dados pessoais – Legítimo Interesse: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia_orientativo_hipoteses_legais_tratamento_de_dados_pessoais_legitimo_interesse
- Guia Orientativo – Tratamento de dados pessoais para fins acadêmicos e para a realização de estudos e pesquisas: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-orientativo-tratamento-de-dados-pessoais-para-fins-academicos-e-para-a-realizacao-de-estudos-e-pesquisas

Lista de medidas

ID	Título, descrição e normas de referência

23.1	**O órgão realiza tratamento de dados pessoais apenas para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público?**

Para cada uma das operações de tratamento de dados pessoais registradas em decorrência do Controle 19, analisar e promover os ajustes para garantir que a organização realiza o tratamento de dados pessoais para o atendimento de finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público.

Normas de referência: Lei nº 13.709/2018, arts. 7º, 11 e 23.

23.2	**O órgão assegura a conformidade das operações às hipóteses de tratamento de dados pessoais (bases legais)?**

Para cada uma das operações de tratamento de dados pessoais registradas em decorrência do Controle 19, analisar o tratamento – quer seja de dado pessoal, dado pessoal sensível ou ambos –, e garantir que a hipótese de tratamento (base legal), disposta no art. 7º ou no art. 11 da Lei nº 13.709/2018, esteja adequada ao caso concreto. Considerar na análise e garantia da conformidade, principalmente, os requisitos da respectiva hipótese de tratamento estabelecidos na Lei nº 13.709/2018, registrando as evidências da análise.

Normas de referência: Lei nº 13.709/2018, arts. 7º e 11.

23.3	**O órgão elabora o Relatório de Impacto à Proteção de Dados Pessoais (RIPD) dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais?**

Para cada uma das operações de tratamento de dados pessoais registradas em decorrência do Controle 19, avaliar se podem gerar riscos às liberdades civis e aos direitos fundamentais dos titulares; em caso positivo, elaborar o RIPD contendo, no mínimo, o disposto na Lei nº 13.709/2018, art. 38, parágrafo único: a descrição dos tipos de dados pessoais coletados; a metodologia aplicada para a coleta e o armazenamento; as medidas adotadas para garantir a segurança das informações; e a análise do controlador quanto aos riscos à privacidade e às salvaguardas implementadas para mitigá-los.

Normas de referência: Lei nº 13.709/2018, arts. 5º, XVII, 10, § 3º, 32 e 38.

23.4	**O órgão, ao realizar estudos em saúde pública, mantém os dados pessoais em ambiente controlado e seguro?**

Na hipótese de a organização ser órgão de pesquisa (conforme disposto no inciso XVIII do art. 5º da Lei nº 13.709/2018), para cada uma das operações de tratamento de dados pessoais registradas em decorrência do Controle 19, identificar a ocorrência de realização de estudos em saúde pública. Para tais operações, promover a implementação de políticas e processos internos, aplicando medidas técnicas para assegurar que os dados pessoais sejam mantidos dentro da organização, em ambiente controlado e seguro, e considerando

os padrões éticos relacionados a estudos e pesquisas, conforme Lei nº 13.709/2018, art. 13. Ademais, anonimizar ou pseudonimizar os dados sempre que possível, e impedir que a divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa revele dados pessoais.

Normas de referência: Lei nº 13.709/2018, art. 13.

23.5 O órgão avalia e aplica medidas para que o tratamento de dados pessoais de crianças e adolescentes ocorra no seu melhor interesse?

Para cada uma das operações de tratamento de dados pessoais registradas em decorrência do Controle 19, avaliar e implementar medidas para garantir que o melhor interesse de crianças e adolescentes ocorra quando do tratamento de seus dados pessoais, conforme Lei nº 13.709/2018, art. 14, e Enunciado n° 1/2023 da ANPD.

Normas de referência: Lei nº 13.709/2018, art. 14; Enunciado n° 1/2023 da ANPD.

23.6 O órgão avalia e aplica medidas para anonimizar os dados pessoais?

Para cada uma das operações de tratamento de dados pessoais registradas em decorrência do Controle 19, aplicar medidas de anonimização de dados pessoais quando necessário, conforme disposto na Lei nº 13.709/2018 e normas complementares.

Normas de referência: Lei nº 13.709/2018, art. 7º,11, 12, 13, 16 e 18.

23.7 O órgão assegura a conformidade do término do tratamento e da eliminação dos dados pessoais?

Para cada uma das operações de tratamento de dados pessoais registradas em decorrência do Controle 19, implementar procedimentos para assegurar o término do tratamento dos dados pessoais, conforme as situações previstas na Lei nº 13.709/2018, art. 15, e sua posterior eliminação, em observância ao disposto no art. 16 quanto à retenção legalmente obrigatória.

Normas de referência: Lei nº 13.709/2018, art. 15 e 16.

6.6 CONTROLE 24: Compartilhamento e transferência internacional

Visão geral

O compartilhamento de dados pessoais com outros agentes de tratamento e as transferências internacionais devem ser submetidas a avaliações específicas sob a égide da LGPD e normas relacionadas. A finalidade é garantir a legalidade dessas operações, considerando as finalidades do tratamento, as medidas de privacidade e de segurança da informação aplicáveis, além dos dispositivos legais e normativos específicos. Incluem-se neste controle a análise prévia da adequação, a aplicação das cláusulas-padrão regulamentares quando cabível e a execução de rotinas obrigatórias de comunicação à ANPD, conforme previsto na legislação.

Por que esse controle é crítico?

Compartilhamentos indevidos sem bases legais ou transferências internacionais sem garantias suficientes ampliam consideravelmente os riscos de exposição indevida e de violação dos direitos dos titulares de dados pessoais. A LGPD e a Resolução CD/ANPD nº 19/2024 estabelecem requisitos para a realização dessas operações, incluindo a necessidade de controles contratuais e técnicos específicos para assegurar a proteção adequada dos dados pessoais.

Procedimentos e ferramentas

Para cada operação de compartilhamento registrada conforme controle 19, é imprescindível realizar, previamente à execução da operação, a análise jurídica e a avaliação dos riscos envolvidos – assegurando a definição clara da base legal aplicável, da compatibilidade com as finalidades do tratamento e da implementação das medidas de proteção necessárias.

Nas transferências internacionais, deve-se confirmar a conformidade mediante a validação das garantias adequadas previstas na Resolução CD/ANPD nº 19/2024, tais como decisão de adequação, cláusulas-padrão contratuais, regras contratuais específicas e obrigações técnicas adicionais. A documentação comprobatória e as cláusulas contratuais que asseguram os direitos dos titulares e as medidas de segurança da informação devem ser mantidas e atualizadas.

Além disso, é necessário instituir procedimentos para a comunicação obrigatória à ANPD quando exigido, garantindo o cumprimento das obrigações legais.

Lista de medidas

ID	Título, descrição e normas de referência
24.1	**O órgão assegura a interoperabilidade dos dados pessoais necessários ao uso compartilhado?**
Para cada uma das operações de tratamento de dados pessoais registradas em decorrência do Controle 19, manter os dados pessoais em formato interoperável e estruturado para o uso compartilhado, nos termos do art. 25 da Lei nº 13.709/2018, do Decreto nº 10.046/2019 e de normas correlatas.	
Normas de referência: Lei nº 13.709/2018, art. 25; Decreto nº 10.046/2019.	
24.2	**O órgão, ao realizar compartilhamento de dados pessoais com outros órgãos e entidades públicos, verifica se o compartilhamento atende a finalidades específicas de execução de políticas públicas e atribuições legais?**
Para cada uma das operações de tratamento de dados pessoais registradas em decorrência do Controle 19, realizar análise dos compartilhamentos de dados pessoais e implementar mecanismos para que as finalidades dos compartilhamentos atendam políticas públicas e	

atribuições legais da organização, em conformidade com a Lei nº 13.709/2018, art. 26 e normas correlatas.

Normas de referência: Lei nº 13.709/2018, art. 26; Decreto nº 10.046/2019.

24.3	**O órgão informa a ANPD ao realizar o compartilhamento de dados pessoais com pessoas jurídicas de direito privado?**

Para cada uma das operações de tratamento de dados pessoais registradas em decorrência do Controle 19, efetuar análise dos compartilhamentos de dados pessoais realizados com pessoas jurídicas de direito privado (controladores) e garantir a conformidade com a Lei nº 13.709/2018, art. 27.

Normas de referência: Lei nº 13.709/2018, art. 27.

24.4	**O órgão comunica os agentes de tratamento, com os quais compartilhou dados pessoais, a correção, a eliminação, a anonimização ou o bloqueio dos referidos dados?**

Para cada uma das operações de tratamento de dados pessoais registradas em decorrência do Controle 19, estabelecer e manter procedimentos para comunicar os agentes de tratamento, com os quais compartilhou dados pessoais, sobre correção, eliminação, anonimização ou bloqueio dos referidos dados, objetivando que tais agentes repitam o procedimento – exceto nos casos em que a comunicação seja comprovadamente impossível ou implique esforço desproporcional.

Normas de referência: Lei nº 13.709/2018, art. 18, § 6º.

24.5	**O órgão observa as regras aplicáveis ao realizar operações de transferência internacional de dados pessoais?**

Para cada uma das operações de tratamento de dados pessoais registradas em decorrência do Controle 19, identificar aquelas que envolvem transferências internacionais de dados pessoais e promover os respectivos ajustes para conformidade ao disposto na Lei nº 13.709/2018 e aos procedimentos e regras estabelecidos na Resolução CD/ANPD nº 19/2024.

Normas de referência: Lei nº 13.709/2018, Capítulo V; Resolução CD/ANPD nº 19/2024.

6.7 CONTROLE 25: Princípios da Lei nº 13.709/2018

Visão geral

A LGPD é considerada uma norma principiológica, ou seja, alicerçada em princípios que estabelecem diretrizes sobre o tratamento de dados pessoais. Além do registro das operações de tratamento de dados pessoais, identificação de hipóteses legais, análises específicas de conformidade do tratamento, incluindo aspectos de compartilhamento e transferência internacional, o tratamento deve observar os princípios previstos na legislação. Dessa forma,

este controle consolida a necessidade de observância dos princípios previstos na LGPD como pilares fundamentais das práticas organizacionais frente ao tratamento de dados pessoais.

Por que esse controle é crítico?

Os princípios da LGPD são norteadores do arcabouço normativo e interpretativo aplicável à proteção de dados pessoais no Brasil. Sua aplicação transcende o mero formalismo legal, influenciando desde o desenho e a implementação dos processos de tratamento até as decisões relativas à retenção, uso e compartilhamento de dados pessoais. A demonstração de aderência efetiva a esses princípios mitiga riscos jurídicos e reputacionais, além de constituir referência essencial para auditorias internas e externas, contribuindo para maior transparência e responsabilidade institucional.

Procedimentos e ferramentas

Recomenda-se a integração sistemática dos princípios em todos os instrumentos normativos e operacionais da organização, incluindo a elaboração de avisos de privacidade, políticas de retenção e minimização de dados pessoais, *checklists* de conformidade aplicados na análise de novos projetos e critérios rigorosos de avaliação em RIPDs. Devem ser instituídos mecanismos de monitoramento que auxiliem na validação efetiva da aplicação dos princípios, como indicadores de transparência, métricas sobre tempo médio de atendimento às solicitações dos titulares e índices de anonimização. A capacitação contínua dos agentes públicos envolvidos nas atividades de conformidade, com conteúdos específicos sobre os princípios e suas aplicações práticas, é igualmente fundamental para assegurar sua ampla disseminação na organização.

Lista de medidas

ID	Título, descrição e normas de referência
25.1	**O órgão realiza tratamento de dados pessoais para propósitos legítimos, específicos, explícitos e informados ao titular?**
Para cada uma das operações de tratamento de dados pessoais registradas em decorrência do Controle 19, analisar se o tratamento é realizado para propósitos legítimos (lícitos, considerando a Lei nº 13.709/2018 e demais legislações aplicáveis), específicos (não devem ser genéricos ou amplos), explícitos (devem ser claros e precisos, evitando qualquer ambiguidade) e informados ao titular (apresentados aos titulares por meio de avisos de privacidade, conforme disposto na medida 25.6).	
Normas de referência: Lei nº 13.709/2018, art. 6º, I, IV e VI.	
25.2	**O órgão realiza o tratamento de dados pessoais de forma compatível com as finalidades informadas ao titular, de acordo com o contexto do tratamento?**
Para cada uma das operações de tratamento de dados pessoais registradas em decorrência do Controle 19, analisar e promover os ajustes para garantir que o tratamento de dados	

pessoais seja compatível com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

Normas de referência: Lei nº 13.709/2018, art. 6º, I, II, IV e VI.

25.3	**O órgão trata somente os dados pessoais necessários para atingir as finalidades?**

Para cada uma das operações de tratamento de dados pessoais registradas em decorrência do Controle 19, a organização deve analisar e promover os ajustes objetivando tratar apenas os dados pessoais estritamente necessários para o cumprimento das finalidades informadas ao titular, abrangendo os dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados pessoais.

Normas de referência: Lei nº 13.709/2018, arts. 6º, III e 7º, III, 10, § 1º, 11, II, b) e 15, I.

25.4	**O órgão assegura aos titulares consulta facilitada e gratuita sobre a forma e a duração do tratamento de seus dados, assim como o acesso aos seus dados pessoais?**

Para cada uma das operações de tratamento de dados pessoais registradas em decorrência do Controle 19, a organização deve garantir consulta facilitada e gratuita sobre a forma e a duração do tratamento dos dados pessoais, em atendimento também à medida 25.6. Ademais, garantir consulta facilitada do titular à integralidade de seus dados pessoais, seja exercendo seu direito de acesso via solicitação ao encarregado (medidas 21.2 e 21.3) ou de forma direta por meio de solução de software.

Normas de referência: Lei nº 13.709/2018, arts. 6º, IV, VI, 9º, 14, § 6º, 18, 19, 20, 23, I, e 33, VIII.

25.5	**O órgão implementa medidas para garantir aos titulares a exatidão, clareza, relevância e atualização dos dados pessoais, de acordo com a necessidade e para cumprir a finalidade do tratamento?**

Para cada uma das operações de tratamento de dados pessoais registradas em decorrência do Controle 19, a organização deve analisar e promover os ajustes para garantir aos titulares que os dados pessoais tratados sejam exatos, claros, relevantes e atualizados, de acordo com a necessidade. Estabelecer processos documentados que possibilitem a revisão e correção de dados pessoais incorretos, incompletos ou desatualizados. Oferecer aos titulares mecanismos, tais como soluções de software, para retificar seus dados. Integrar validações automáticas e manuais nos sistemas para melhorar a precisão dos dados pessoais tratados.

Normas de referência: Lei nº 13.709/2018, arts. 6º, V, VII, 46, 47 e 49.

25.6	**O órgão assegura aos titulares informações claras, precisas e facilmente acessíveis sobre os tratamentos de dados pessoais?**

Para cada uma das operações de tratamento de dados pessoais registradas em decorrência do Controle 19, a organização deve analisar a necessidade de elaborar avisos de privacidade. Tais avisos devem conter informações claras, precisas e facilmente acessíveis aos titulares sobre as operações de tratamento de dados pessoais realizadas, inclusive atendendo à necessidade de as informações serem compreensíveis ao público-alvo, eventualmente não familiarizado com as tecnologias da informação, internet ou jargões jurídicos. Recomenda-se que os avisos de privacidade contemplem minimamente as informações dispostas na Lei nº 13.709/2018, art. 9º e art. 23, I, além da Resolução CD/ANPD nº 19/2024, Anexo, art. 17, § 2º; e, para o tratamento de dados pessoais sensíveis, considerar a Lei nº 13.709/2018, art. 11, § 2º. Ademais, nas situações em que o tratamento envolver dados pessoais de crianças e adolescentes, considerar a Lei nº 13.709/2018, art. 14, § 6º.

Normas de referência: Lei nº 13.709/2018, arts. 6º, VI, 9º, 14, § 6º, 18, 19, 20, 23, I, e 33, VIII.

25.7 O órgão implementa medidas técnicas e administrativas aptas a proteger os dados pessoais?

Para cada uma das operações de tratamento de dados pessoais registradas em decorrência do Controle 19, a organização deve implementar medidas técnicas e administrativas para proteger os dados pessoais contra acessos não autorizados; situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; vazamentos e outros tipos de incidentes (também em atendimento à medida 25.8).

Normas de referência: Lei nº 13.709/2018, arts. 6º, VII, 46, 47 e 49.

25.8 O órgão implementa medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais?

Para cada uma das operações de tratamento de dados pessoais registrada em decorrência do Controle 19, a organização deve implementar mecanismos de mitigação de riscos e medidas que previnam a ocorrência de danos no tratamento de dados pessoais (também em razão da medida 0.17). Para os tratamentos que possam gerar riscos às liberdades civis e aos direitos fundamentais, elaborar relatórios de impactos à proteção de dados pessoais (RIPD), igualmente em atendimento à medida 23.3. Estabelecer procedimento ou metodologia para assegurar a privacidade desde a fase de concepção do produto ou do serviço até a sua execução, conforme previsto na medida 20.4.

Normas de referência: Lei nº 13.709/2018, art. 6º, V, VIII, e 46.

25.9 O órgão assegura que o tratamento de dados pessoais não seja realizado para fins discriminatórios ilícitos ou abusivos?

Para cada uma das operações de tratamento de dados pessoais registradas em decorrência do Controle 19, analisar e promover ajustes para garantir que o tratamento de dados

pessoais não seja realizado para fins discriminatórios, ilícitos ou abusivos, inclusive nos tratamentos automatizados de dados pessoais.

Normas de referência: Lei nº 13.709/2018, art. 6º, IX, e 20, § 2º.

25.10	**O órgão adota medidas de responsabilização e prestação de contas, capazes de evidenciar o cumprimento das normas de proteção de dados pessoais?**

Garantir que todas as medidas implementadas com o objetivo de assegurar a conformidade às normas de proteção de dados pessoais sejam devidamente evidenciadas, de forma sistemática e auditável, registrando inclusive a eficácia das medidas. Isto inclui o registro de evidências tais como: o PGP; o registro das operações de tratamento e as respectivas ações para conformidade; as solicitações formuladas pelos agentes públicos ao encarregado e suas respectivas orientações; o atendimento aos direitos dos titulares; os RIPDs; as ações de conscientização e de treinamento; o relatório anual contemplando indicadores que sintetizem as ações adotadas para assegurar a conformidade às normas protetivas de dados pessoais, incluindo controles e medidas do PPSI; entre outros.

Normas de referência: Lei nº 13.709/2018, art. 6º, X, e 50.

7 Considerações finais

A concepção do *framework* do PPSI 2.0 direcionado especificamente aos órgãos e entidades da Administração Pública federal direta, autárquica e fundacional, que possuem unidades integrantes do SISP, representa um marco fundamental para a consolidação e fortalecimento da governança em privacidade e segurança da informação no setor público nacional. Sua criação fundamentou-se nas necessidades reais e nas particularidades deste contexto, integrando as melhores práticas internacionais e, simultaneamente, atendendo às exigências da legislação brasileira vigente, em especial a LGPD e demais normativos da ANPD, bem como as diretrizes do GSI/PR. A estratégia adotada para seu desenvolvimento envolveu ampla pesquisa, mapeamento normativo e consulta a especialistas, garantindo que o *framework* seja ao mesmo tempo robusto, flexível e aplicável às diversas realidades institucionais do setor público federal.

A transformação digital dos serviços públicos é uma realidade no âmbito das organizações públicas brasileiras, demandando uma estrutura de governança que permeie toda organização. Nesse sentido, ressalta-se que o comprometimento da alta administração representa fator crítico de sucesso para a implementação do *framework* do PPSI 2.0.

Este guia apresenta uma estrutura clara e organizada, dividida em segmentos que contemplam desde a estruturação básica para governança, passando pelos instrumentos fundamentais, até os controles de segurança da informação e privacidade. Cada controle é detalhado com uma visão geral, a justificativa de sua criticidade, e os procedimentos e ferramentas recomendados para facilitar sua adoção pelas organizações públicas. Essa arquitetura permite que as instituições mapeiem e acompanhem as ações necessárias para o aprimoramento contínuo de suas práticas, conciliando conformidade legal, maturidade técnica e resiliência operacional.

Por fim, ressalta-se o objetivo central deste guia e do *framework* do PPSI 2.0: auxiliar os órgãos do SISP na construção de um ambiente organizacional seguro, transparente e conforme os preceitos legais, promovendo a proteção dos dados pessoais dos cidadãos e o fortalecimento da confiança nas instituições públicas. A utilização deste documento como referência e suporte técnico contribuirá decisivamente para a concretização de políticas efetivas de governança em privacidade e segurança da informação, elevando o padrão das práticas no setor público e apoiando a conformidade com as normas vigentes.

8 Referências

[1] CENTER FOR INTERNET SECURITY. **CIS Controls Guide, versão 8.1.** Março de 2025. Disponível em: https://www.cisecurity.org/controls. Acesso em: 16 out. 2025.

[2] **Secure Controls Framework**. Secure Controls Framework, 2025. Disponível em: https://securecontrolsframework.com/. Acesso em: 16 out. 2025.

[3] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27001:2023**: Segurança da informação, segurança cibernética e proteção à privacidade — Sistemas de gestão da segurança da informação — Requisitos. Rio de Janeiro, 2023.

[4] _____. **ABNT NBR ISO/IEC 27002:2023**: Segurança da informação, segurança cibernética e proteção à privacidade — Controles de segurança da informação. Rio de Janeiro, 2023.

[5] International Organization for Standardization. **ISO/IEC 27701:2025** – Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines. ISO; 2025.

[6] CENTER FOR INTERNET SECURITY. **CIS Controls v8 Privacy Companion Guide, versão 8**. Janeiro de 2022. Disponível em: https://www.cisecurity.org/insights/white-papers/cis-controls-v8-privacy-companion-guide. Acesso em: 17 out. 2025.

[7] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Cybersecurity Framework 2.0**. Gaithersburg, MD: NIST, 2024. Disponível em: https://doi.org/10.6028/NIST.CSWP.29. Acesso em: 17 out. 2025.

[8] _____. **NIST Privacy Framework: a tool for improving privacy through enterprise risk management, version 1.0**. Gaithersburg, MD: NIST, 2020. Disponível em: https://doi.org/10.6028/NIST.CSWP.01162020. Acesso em: 17 out. 2025.

[9] BRASIL. Presidência da República. Gabinete de Segurança Institucional. Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021. **Processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal.** Brasília, DF: GSI/PR, 2021. Disponível em: https://www.in.gov.br/en/web/dou/-/instrucao-normativa-gsi/pr-n-3-de-28-de-maio-de-2021-322963172. Acesso em: 17 out. 2025.

[10] CENTER FOR INTERNET SECURITY. **CIS Controls Clould Companion Guide, versão 8.1.** Dezembro de 2024. Disponível em: https://www.cisecurity.org/insights/white-papers/cis-controls-v8-1-cloud-companion-guide. Acesso em: 17 out. 2025.

[11] BRASIL. Ministério da Justiça e Segurança Pública. Agência Nacional de Proteção de Dados. Resolução CD/ANPD nº 15, de 24 de abril de 2024. **Regulamento de Comunicação de Incidente de Segurança.** Brasília, DF: ANPD, 2024. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024. Acesso em: 17 out. 2025.

[12] _____. Resolução CD/ANPD nº 18, de 16 de julho de 2024. **Regulamento sobre a atuação do encarregado pelo tratamento de dados pessoais.** Brasília, DF: ANPD, 2024. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-18-de-16-de-julho-de-2024-572632074. Acesso em: 17 out. 2025.

[13] _____. Resolução CD/ANPD nº 19, de 23 de agosto de 2024. **Regulamento de Transferência Internacional de Dados e o conteúdo das cláusulas-padrão contratuais.** Brasília, DF: ANPD, 2024. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-19-de-23-de-agosto-de-2024-580095396. Acesso em: 17 out. 2025.

[14] _____. **Guia Orientativo - Tratamento de Dados Pessoais pelo Poder Público versão 2.0**. Junho de 2023. Brasília, DF: ANPD, 2023. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia_orientativo_tratamento_de_dados_pessoais_pelo_poder_publico. Acesso em: 17 out. 2025.

gov.br

Dúvida?

Entre em contato conosco

Formulário:
https://forms.office.com/r/j8w0h9Mvi1

Email:
ppsi.sgd@gestao.gov.br

Telefone:
(61) 2020-2046

MINISTÉRIO DA
GESTÃO E DA INOVAÇÃO
EM SERVIÇOS PÚBLICOS

GOVERNO DO
BRASIL
DO LADO DO POVO BRASILEIRO