# Cartilha da Estrutura de Governança do PPSI

Programa de Privacidade e Segurança da Informação
**PPSI 2.0**

**Versão 1.0**
**Brasília, 20 de janeiro de 2026**

MINISTÉRIO DA
GESTÃO E DA INOVAÇÃO
EM SERVIÇOS PÚBLICOS

GOVERNO DO BRASIL
DO LADO DO POVO BRASILEIRO

**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 Revisora**
Marta Juvina de Medeiros
Ricardo Borges Almeida

## Introdução

Esta cartilha compõe o conjunto de documentos orientativos elaborados no âmbito do *Framework* de Privacidade e Segurança da Informação do Programa de Privacidade e Segurança da Informação (PPSI 2.0), elaborado pela Secretaria do Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos.

O objetivo deste documento é apresentar de forma clara e didática os papéis e responsabilidades previstos no *framework*, no intuito de facilitar a preparação dos 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).

Para cada papel integrante da estrutura de governança, apresenta-se uma breve contextualização por meio de uma síntese fundamentada nas referências normativas, seguida de sugestões práticas e objetivas, com o propósito de proporcionar uma compreensão clara e simplificada destas medidas previstas no *framework*. Dessa forma, pretende-se apoiar a implementação eficaz das ações do Programa, contribuindo para o fortalecimento da maturidade e da resiliência em privacidade e segurança da informação no âmbito dos órgãos do SISP.

## Alta Administração

A Alta Administração deve estabelecer, manter, monitorar e aprimorar o **sistema de gestão de riscos e controles internos** da organização, 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, 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 cibernéticos.

---

**Referências:**

- Decreto nº 9.203/2017, art. 17.
- Portaria SGD/MGI nº 9.511/2025, arts 7º e 8º.
- Acórdão TCU nº 2387/2024 – Plenário.

**Decreto nº 9.203/2017, art. 17**

*Art. 17. A alta administração das organizações da administração pública federal direta, autárquica e fundacional deverá estabelecer, manter, monitorar e aprimorar sistema de gestão de riscos e controles internos com vistas à identificação, à avaliação, ao tratamento, ao monitoramento e à análise crítica de riscos que possam impactar a implementação da estratégia e a consecução dos objetivos da organização no cumprimento da sua missão institucional...*

**Portaria SGD/MGI nº 9.511/2025, art. 8º**

*Art. 8º À alta administração compete gerir os riscos no âmbito organizacional, fornecer os recursos necessários para assegurar a gestão da privacidade e da segurança da informação, viabilizar a implementação da estrutura de governança do PPSI e adotar decisões sobre privacidade e segurança da informação em um nível de relevância e prioridade adequadas e alinhadas com a estratégia e com a consecução dos objetivos do órgão ou entidade no cumprimento da sua missão institucional.*

## Alta Administração

### Exemplos de implementação

**1. Estrutura formal de gestão de riscos**

Estabelecimento de estrutura formal de gestão de riscos que inclua representação da alta administração das áreas de tecnologia, segurança da informação e proteção de dados pessoais.

Atribuição clara de papéis e responsabilidades em norma interna garantindo que os gestores de processo reportem periodicamente à alta administração sobre riscos identificados e planos de tratamento.

**2. Liderança pelo exemplo**

A alta administração deve exercer a liderança pelo exemplo, demonstrando comprometimento efetivo com as políticas, normas e procedimentos institucionais de privacidade e segurança da informação. Isso implica cumprir integralmente as regras estabelecidas e evitar a criação de exceções para si ou para suas unidades, assegurando que todos os níveis hierárquicos estejam sujeitos aos mesmos padrões de conduta e controles internos.

Na prática, essa postura se traduz em ações como:

- utilização exclusiva dos canais e sistemas oficiais para tratamento de dados institucionais, observando as diretrizes de classificação, acesso e uso seguro dos dados;
- participação ativa em campanhas internas de conscientização, reforçando junto às equipes a importância da conformidade com as políticas aprovadas;
- aprovação e acompanhamento rigoroso das normas emanadas pelos comitês de governança, riscos, privacidade e segurança da informação, garantindo que não haja tolerância com desvios de conduta ou descumprimento;
- comunicação institucional da alta gestão reiterando que o exemplo vem do topo e que o cumprimento das políticas de privacidade e segurança da informação é uma responsabilidade coletiva e inegociável.

Essa prática contribui para consolidar a cultura de integridade, responsabilidade e conformidade, fortalecendo a credibilidade das ações da alta administração e estimulando a adesão dos servidores às diretrizes internas.

## Gestor de TIC

O órgão ou entidade deve 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 (TIC), conforme atribuições previstas no inciso IV do art. 4º da Portaria nº 778/2019 e em demais normas correlatas.

O gestor de TIC possui papel central na administração dos riscos relacionados às tecnologias adotadas pelo órgão ou entidade. Entre suas principais responsabilidades, destaca-se o compromisso com a integração da segurança da informação desde a concepção dos projetos tecnológicos, bem como a promoção consistente da cultura de privacidade e segurança da informação entre os agentes públicos da sua unidade, alinhando-se às boas práticas de governança e conformidade normativa.

**Referências:**

- Portaria SGD/ME nº 778/2019.
- Portaria SGD/MGI nº 9.511/2025, arts 7º e 9º.

**Portaria SGD/ME nº 778/2019**

*Art. 4º Visando atender aos princípios descritos nesta Portaria, os órgãos e entidades pertencentes ao SISP deverão observar as seguintes diretrizes:*

*[...]*

*IV - o gestor de TIC é responsável pelo planejamento, desenvolvimento, execução e monitoramento das atividades de TIC, devendo assessorar o Comitê de Governança Digital na governança de TIC, provendo todas as informações de gestão para a tomada de decisão das instâncias superiores;*

*[...]*

**Portaria SGD/MGI nº 9.511/2025, art. 9º**

*Art. 9º Ao gestor de tecnologia da informação e comunicação compete planejar, desenvolver, executar e monitorar as medidas de privacidade e segurança da informação em soluções de tecnologia da informação e comunicação, considerando inclusive a cadeia de suprimentos relacionada à solução.*

## Gestor de TIC

### Exemplos de implementação

#### 1. Integração à Governança Institucional

Para além da indicação formal do titular e substituto, a inclusão do gestor de TIC como membro permanente dos comitês de governança digital, segurança da informação e privacidade, ou estruturas equivalentes, contribui para visão técnica nos processos decisórios.

Outro aspecto relevante é o estabelecimento de fluxos formais de comunicação entre o gestor de TIC, o gestor de segurança da informação, o encarregado pelo tratamento de dados pessoais, o responsável pela gestão da integridade, bem como com a alta administração, além de demais partes interessadas na promoção das ações de privacidade e segurança da informação.

#### 2. Planejamento e implementação de medidas de privacidade e segurança da informação

O gestor de TIC deve elaborar e manter atualizado um plano de ações voltado à implementação das medidas de privacidade e segurança da informação relacionadas às soluções tecnológicas da organização. Isto também inclui a avaliação de fornecedores e prestadores de serviços de TIC. Esse plano deve estabelecer metas, prazos e responsáveis, a fim de assegurar a execução coordenada das iniciativas previstas no PPSI.

Para fins de monitoramento, o gestor de TIC pode utilizar instrumentos formais de acompanhamento, tais como painéis em ferramentas corporativas ou planos de ação registrados no sistema de processos administrativos, garantindo a rastreabilidade da execução.

Periodicamente, recomenda-se que o gestor de TIC elabore relatórios técnicos destinados aos comitês competentes e à alta administração, contendo a análise do avanço das ações, o alcance das metas, a identificação de eventuais desvios e a proposição das medidas corretivas necessárias. Dessa forma, assegura-se uma gestão contínua, transparente e alinhada às diretrizes institucionais de governança, privacidade e segurança da informação.

## Gestor de Segurança da Informação

O órgão ou entidade deve designar formalmente um titular e seu respectivo substituto, escolhidos entre servidores públicos civis ocupantes de cargo efetivo ou militares de carreira, que possuam formação ou capacitação técnica compatível com as atribuições do cargo, para o exercício da função de gestor de segurança da informação. A sua atuação deve observar as atribuições estabelecidas no art. 19 da Instrução Normativa nº 1/2020, do Gabinete de Segurança Institucional da Presidência da República (GSI/PR), bem como demais normas aplicáveis.

**Referências:**

- Decreto nº 12.572, de 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
- Portaria SGD/MGI nº 9.511/2025, arts 7º e 10.

**Portaria SGD/MGI nº 9.511/2025, art. 10**

*Art. 10. Ao gestor de segurança da informação compete conduzir o diagnóstico de segurança da informação, bem como orientar, planejar e monitorar as medidas de segurança da informação.*

**IN GSI/PR nº 1/2020**

*Art. 19. Ao Gestor de Segurança da Informação dos órgãos e das entidades da administração pública federal compete [...]:*

*I - coordenar as iniciativas de segurança da informação [...];*

*II - estimular iniciativas de capacitação em temas relacionados à segurança da informação e promover ações de conscientização [...];*

*III - divulgar as normas internas de segurança da informação [...];*

*IV - realizar avaliações de riscos e análise dos impactos [...];*

*V - planejar e propor os recursos orçamentários [...];*

*VI - acompanhar os trabalhos da ETIR;*

*VII - atuar como segunda linha de defesa no âmbito do Sistema de Controle Interno;*

*VIII - realizar avaliações de conformidade [...];*

*IX - acompanhar a aplicação de ações corretivas e administrativas [...];*

*X - cooperar com o Encarregado pelo Tratamento de Dados Pessoais [...];*

*XI - elaborar e revisar o planejamento tático de segurança da informação, [...];*

*XII - participar de fóruns especializados [...]; e*

*XIII - avaliar a capacidade operacional do órgão ou da entidade que representa, a fim de: [...].*

## Gestor de Segurança da Informação

### Exemplos de implementação

#### 1. Articulação com a alta administração e comitês

O gestor deve atuar como ponto focal da alta administração para temas de segurança da informação, apresentando diagnósticos, riscos identificados, necessidades de recursos e recomendações. Também é apropriado que o gestor participe das reuniões dos comitês de governança, riscos, segurança da informação e privacidade, fornecendo subsídios para decisões estratégicas que envolvam a temática.

#### 2. Promoção do conhecimento sobre segurança da informação

Dentre os maiores desafios da segurança da informação estão a necessidade de qualificação, bem como a de conscientização do elemento humano. Nesta perspectiva, o gestor de segurança da informação pode promover ações de capacitação técnica para servidores que atuam em temas relacionados à segurança da informação, assegurando o desenvolvimento das competências necessárias. Tais ações incluem desde orientações pontuais, como referências para aprimorar um ciclo de desenvolvimento de software seguro, sugestões de cursos, e até mesmo a criação de treinamentos formais.

Além disso, o gestor pode promover a implementação de iniciativas de conscientização alinhadas à Norma Complementar nº 18/IN01/DSIC/GSIPR, por meio de campanhas, materiais informativos e comunicações internas que reforcem boas práticas e o uso seguro das informações e dos recursos tecnológicos.

## Encarregado

O **encarregado pelo tratamento de dados pessoais**, e seu respectivo substituto, devem ser designados formalmente 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. Para esta designação, o órgão também deve considerar a **IN SGD/ME nº 117/2020**.

Neste sentido, cumpre destacar que o encarregado atua como ponto de contato entre o órgão ou entidade, os titulares e a ANPD, sendo responsável por receber e tratar reclamações, comunicações e solicitações relacionadas à proteção de dados pessoais. Também orienta agentes públicos sobre as práticas adequadas de privacidade. Além disso, conduz o diagnóstico de privacidade, realizando a interlocução com demais áreas do órgão ou entidade para coleta das informações necessárias.

**Referências:**

- Lei nº 13.709/2018, arts. 23, III e 41
- Resolução CD/ANPD nº 18/2024, arts. 3º, 4º ,5º e 7º
- Instrução Normativa SGD/ME nº 117, de 19 de novembro 2020
- Portaria SGD/MGI nº 9.511/2025, arts. 7º e 11.

**Lei nº 13.709/2018**

*Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.*

*[...]*

*§ 2º As atividades do encarregado consistem em:*

*I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;*

*II - receber comunicações da autoridade nacional e adotar providências;*

*III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e*

*IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.*

*[...]*

**Portaria SGD/MGI nº 9.511/2025, art. 11**

*Art. 11. Ao encarregado pelo tratamento de dados pessoais compete conduzir o diagnóstico de privacidade, bem como orientar os agentes de tratamento no planejamento, implementação e monitoramento das medidas de privacidade.*

## Encarregado

### Exemplos de implementação

#### 1. Estabelecimento de fluxo para orientações aos agentes públicos

O órgão estabelece um fluxo formal para que agentes públicos encaminhem dúvidas, solicitações de orientação e comunicações relacionadas ao tratamento de dados pessoais ao encarregado. Esse fluxo — estruturado em canal institucional, com registro e rastreabilidade — assegura atendimento organizado e tempestivo, além de permitir que o encarregado consolide informações e identifique necessidades recorrentes de orientação.

Tal procedimento está alinhado ao art. 10, II, da Resolução CD/ANPD nº 18/2024, ao promover meior para que os agentes públicos solicitem assistência e orientação do encarregado sempre que realizarem atividades de tratamento ou tomarem decisões estratégicas relacionadas ao tratamento de dados pessoais, fortalecendo a governança e a conformidade com a LGPD.

#### 2. Definição de processo para atendimento dos direitos dos titulares

O encarregado pelo tratamento de dados pessoais deve, com apoio das unidades competentes e da alta administração, implantar e gerenciar um canal institucional formalizado para receber solicitações, dúvidas, reclamações e comunicações dos titulares de dados pessoais. Esse canal, que pode incluir formulário eletrônico, sistema de chamados, entre outros meios tecnológicos, deve garantir a autenticação do titular, o registro, a rastreabilidade e o atendimento eficiente de todas as demandas, permitindo controle e acompanhamento das providências adotadas.

Para assegurar a efetividade do atendimento, o procedimento deve prever a participação ativa das unidades administrativas do órgão ou entidade, garantindo o pronto apoio necessário para o fornecimento das informações solicitadas pelos titulares de forma alinhada ao art. 3º, inciso II, da IN SGD/ME nº 117/2020.

Dessa forma, o fluxo formal de atendimento não apenas organiza a interlocução com os titulares, mas também fortalece a governança de privacidade e a integração entre o encarregado e as diversas áreas do órgão ou entidade.

## Responsável Setorial pela Gestão da Integridade

Servidor responsável pela gestão da integridade na organização, nos termos do disposto no **art. 5º, II do Decreto nº 11.529/2023**.

No **âmbito do PPSI**, em conformidade as disposições previstas no art. 12 da Portaria SGD/MGI nº 9.511/2025, atua na realização do diagnóstico das medidas de estruturação básica para governança e de instrumentos fundamentais, bem como exerce a coordenação e a gestão dos riscos à integridade correlatos aos temas tratados.

**Referências:**

- Decreto nº 11.529, de 16 de maio de 2023, art. 5º, II
- Portaria SGD/MGI nº 9.511/2025, arts. 7º e 12.

**Decreto 11.529/2023**

*Art. 5º Compõem o Sitai:*

*I - a Controladoria-Geral da União, como órgão central; e*

*II - as unidades nos órgãos e nas entidades da administração pública federal direta, autárquica e fundacional responsáveis pela gestão da integridade, da transparência e do acesso à informação, como unidades setoriais.*

*[...]*

**Portaria SGD/MGI nº 9.511/2025, art. 12**

*Art. 12. Ao responsável setorial pela gestão da integridade compete o diagnóstico das medidas relativas à estruturação básica e instrumentos fundamentais de governança do PPSI, além da coordenação e gestão dos riscos para a integridade relacionados aos temas.*


## Exemplos de implementação

### 1. Fornecimento de apoio metodológico

Considerando seu papel e experiência na condução dos programas de integridade, em articulação com o encarregado pelo tratamento de dados pessoais, com o gestor de segurança da informação e com o gestor de TIC, o responsável setorial pela gestão da integridade pode compartilhar seu conhecimento e fornecer suporte metodológico aos diagnósticos temáticos (privacidade, segurança da informação, tecnologia, continuidade, entre outros), orientando as áreas sobre classificação de maturidade, eventual coleta de evidências para subsidiar a análise interna, critérios organizacionais para priorização de ações, entre outros aspectos.

Dessa forma, o responsável setorial pela gestão da integridade também promove a articulação contínua entre as áreas envolvidas no PPSI, incluindo a alta administração, podendo realizar reuniões regulares para apoiar o andamento das ações, esclarecer dúvidas e assegurar o alinhamento das medidas de privacidade e segurança da informação. Isso contribui para a implementação coordenada e coerente do Programa.

### 2. Integração da gestão de riscos institucionais ao PPSI

O responsável setorial pela gestão da integridade pode atuar como articulador entre as áreas envolvidas no PPSI e a estrutura institucional de gestão de riscos, promovendo a integração entre os riscos de privacidade e segurança da informação com o modelo de riscos da organização. Essa articulação pode incluir a facilitação de reuniões entre gestores de riscos e responsáveis pelas medidas do PPSI, a promoção do alinhamento metodológico entre os instrumentos do PPSI e a matriz institucional de riscos, e o apoio à definição de critérios uniformes de avaliação, priorização e registro dos riscos relacionados ao Programa.

Além disso, pode auxiliar na consolidação das informações encaminhadas pelas áreas, garantindo que os riscos identificados no âmbito do PPSI sejam comunicados às instâncias competentes e adequadamente refletidos nos instrumentos de governança e integridade. Dessa forma, o responsável contribui para que o PPSI seja implementado de maneira coerente com o sistema de gestão de riscos do órgão, sem assumir competências técnicas próprias das áreas finalísticas, mas fortalecendo a coordenação e a interoperabilidade entre elas.

## Comitê de Segurança da Informação

O **Comitê de Segurança da Informação** ou estrutura equivalente é responsável por deliberar sobre os assuntos relativos à **Política Nacional de Segurança da Informação** e **normas de segurança da informação**, contemplando as demais atribuições do **art. 20 da IN GSI/PR nº 1/2020**.

Além disso, **no âmbito do PPSI**, o **Comitê de Segurança da Informação** possui papel fundamental na definição de estratégias para elaboração e divulgação dos instrumentos fundamentais de governança atinentes à área de segurança da informação, além de fornecer apoio para demais medidas previstas no PPSI sobre o tema. Isto pode incluir a definição de grupos de trabalho para elaboração dos instrumentos, além dos demais trâmites considerando seu papel deliberativo.

**Referências:**

- Lei nº 13.709/2018, arts. 6º, incisos VII e VIII, 46 e 50.
- Decreto nº 12.572, de 2025, art. 10, II.
- Instrução Normativa GSI/PR nº 1/2020, art. 16, II e Capítulo VI, Seção II.
- Instrução Normativa GSI/PR nº 3/2021, art. 45.

**IN GSI/PR nº 1/2020, art. 20**

*Art. 20. O Comitê de Segurança da Informação interno dos órgãos e das entidades da administração pública federal possui as seguintes atribuições:*

*I - assessorar a implementação das ações de segurança da informação;*

*II - constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação;*

*III - participar da elaboração da Política de Segurança da Informação e das normas internas de segurança da informação;*

*IV - propor alterações à Política de Segurança da Informação e às normas internas de segurança da informação;*

*V - deliberar sobre normas internas de segurança da informação; e*

*VI - deliberar sobre as ações propostas pelo gestor de segurança da informação no parecer técnico sobre o relatório de avaliação de conformidade e encaminhar à alta administração para aprovação o processo contendo os documentos sobre a avaliação de conformidade.*

## Comitê de Segurança da Informação

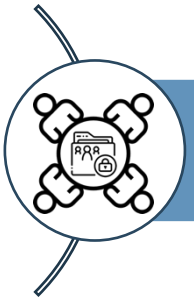
### Exemplos de implementação

#### 1. Definição de estratégia e coordenação para elaboração dos instrumentos fundamentais

O Comitê pode atuar na definição da abordagem metodológica e das responsabilidades das áreas envolvidas na elaboração dos instrumentos fundamentais de governança de segurança da informação propostos no framework do PPSI 2.0, para além das políticas, normas e procedimentos internos, aprovando cronogramas, emitindo orientações e definindo critérios mínimos de conteúdo. Também pode instituir grupos de trabalho especializados para elaborar ou revisar tais instrumentos, acompanhando a execução e deliberando sobre versões finais antes de submetê-las à alta administração.

#### 2. Apoio ao gestor de segurança da informação no diagnóstico do PPSI

No âmbito do PPSI, o Comitê pode analisar os diagnósticos produzidos pelo gestor de segurança da informação, avaliar lacunas, riscos e recomendações e deliberar sobre as ações propostas. Essa avaliação pode resultar em ajustes no plano de trabalho, priorização de iniciativas, solicitação de informações adicionais ou encaminhamento de temas estratégicos à alta administração para deliberação final.



## Comitê de Proteção de Dados Pessoais

O órgão ou entidade deve 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. O Comitê desempenha papel fundamental na consolidação da governança de privacidade e no fortalecimento da atuação do encarregado pelo tratamento de dados pessoais.

Além disso, **no contexto do PPSI**, o **Comitê** desempenha papel essencial na estruturação e manutenção das medidas do *framework* relacionadas aos instrumentos fundamentais de governança da privacidade, sendo responsável pela avaliação da necessidade e instituição de grupos de trabalho, bem como pela elaboração, deliberação e atualização das políticas, normas e procedimentos internos relacionados à proteção de dados pessoais.

**Referências:**

- Lei nº 13.709/2018, art. 50.
- Resolução CD/ANPD nº 18/2024, art. 10, inciso V.

**Lei nº 13.709/2018**

*Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.*

**Resolução CD/ANPD nº 18/2024**

*Art. 10. O agente de tratamento deverá*

*[...]*

*V - garantir ao encarregado acesso direto às pessoas de maior nível hierárquico dentro da organização, aos responsáveis pela tomada de decisões estratégicas que afetem ou envolvam o tratamento de dados pessoais, bem como às demais áreas da organização.*


## Exemplos de Implementação

### 1. Integração do Comitê ao ciclo de governança do PPSI

O diagnóstico do PPSI, conduzido pelo encarregado, pode ser apresentado periodicamente ao Comitê de Proteção de Dados Pessoais como parte do fluxo de governança do programa. O Comitê, como instância deliberativa, pode receber o diagnóstico, discutir riscos institucionais, indicar prioridades e determinar encaminhamentos estratégicos, garantindo que as recomendações do encarregado sejam analisadas e respaldadas pela alta administração.

Durante as reuniões, o encarregado tem acesso direto aos gestores de maior nível hierárquico e às áreas responsáveis por decisões estratégicas de tratamento de dados pessoais, conforme previsto no art. 10, V da Resolução CD/ANPD nº 18/2024.
Esse processo fortalece a governança interna, assegura que o diagnóstico do encarregado tenha efeitos concretos na tomada de decisão e permite que o PPSI seja conduzido como política contínua e integrada ao planejamento da instituição.

### 2. Instituição de grupos de trabalho temáticos para desenvolvimento e revisão dos instrumentos fundamentais de governança

Com base no diagnóstico do PPSI apresentado pelo encarregado e nas deliberações do Comitê, podem ser instituídos Grupos de Trabalho (GTs) para tratar temas específicos e apoiar a implementação das medidas de privacidade do órgão, incluindo o desenvolvimento e revisão dos instrumentos fundamentais de governança, conforme necessidades identificadas no diagnóstico do PPSI. Esses GTs reúnem representantes das áreas envolvidas no tratamento de dados pessoais e atuam com escopo delimitado, cronograma e entregáveis específicos, como minutas de políticas, revisões de procedimentos, análises de riscos ou propostas de melhoria.
Os GTs reportam seu andamento ao Comitê, que avalia as entregas, delibera sobre sua aprovação e define sua incorporaçãO às políticas e normas internas. Essa estrutura permite que ações de privacidade sejam conduzidas de forma colaborativa, técnica e alinhada às prioridades estratégicas da organização.

## ETIR

A **Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR)** deve ser instituída por todos os órgãos e entidades que possuem a competência de administrar a infraestrutura de rede de sua organização, sendo composta, preferencialmente, por servidores públicos civis ocupantes de cargo efetivo ou militares, com capacitação técnica compatível com as atividades da equipe. A composição deve prever um substituto para cada membro da equipe.

Para regulamentar a atuação da equipe, deve ser elaborado o documento de constituição da ETIR conforme **NC n° 05/IN01/DSIC/GSIPR**, devidamente aprovado pela alta administração do órgão.

**IN GSI/PR nº 1/2020**

*Art. 15. Além das obrigações já dispostas nesta Instrução Normativa, compete aos órgãos e às entidades da administração pública federal, direta e indireta, em seu âmbito de atuação:*

*[...]*

*IV - instituir e implementar Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR, que constituirá a rede de equipes, integrada pelos órgãos e pelas entidades da administração pública federal, coordenada pelo Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo do Gabinete de Segurança Institucional da Presidência da República;*

*[...]*

**NC n° 05/IN01/DSIC/GSIPR**

*6.2 Recomenda-se como missão prioritária para a Equipe a facilitação e a coordenação das atividades de tratamento e resposta a incidentes em redes computacionais, além de alguma outra missão específica, em consonância com as atividades de resposta e tratamento a incidentes em redes, tais como: recuperação de sistemas, análise de ataques e intrusões, cooperação com outras equipes, participação em fóruns e redes nacionais e internacionais.*

---

**Referências:**

- Lei nº 13.709/2018, arts. 6º, VII e VIII, 46, 48 e 50, § 2º, I, g.
- Decreto nº 12.572/2025.
- Decreto nº 10.748, de 16 de julho de 2021.
- Decreto nº 9.203/2017 art. 2º, IV.
- Instrução Normativa GSI/PR nº 1/2020, art. 15, IV.
- Resolução CD/ANPD nº 15/2024.
- Norma Complementar n° 05/IN01/DSIC/GSIPR.

## ETIR

### Exemplos de implementação

#### 1. Construção de fluxo integrado de tratamento e resposta a incidentes

A ETIR elabora proposta de procedimento para gestão de incidentes de segurança da informação que engloba: (i) canais para notificação de incidentes; (ii) classificação inicial; (iii) procedimentos de contenção, erradicação e recuperação; (iv) registros e evidências; (v) comunicação com áreas internas e externas.
No caso de incidentes com dados pessoais, prever os meios de comunicação do incidente ao encarregado pelo tratamento de dados pessoais, e respecitva comunicação à ANPD, quando aplicável. Desta forma, o fluxo proposto deve garantir a participação de todas as partes interessadas, desde o gestor de TIC, o gestor de segurança da informação, o encarregado pelo tratamento de dados pessoais, até os gestores de unidades impactadas pelo incidente. O documento deve ser submetido aos diferentes comitês envolvidos.

#### 2. Realização de exercícios simulados de incidentes

A ETIR organiza exercícios simulados de tratamento de incidentes como mecanismo de validação contínua da capacidade institucional de reação a eventos de privacidade e segurança da informação. Esses exercícios podem ser realizados em diferentes formatos — como tabletop, simulações técnicas controladas ou exercícios híbridos — e envolvem múltiplas áreas da organização.
Ao final das simulações, a ETIR consolida um relatório com o desempenho das equipes, os tempos de resposta, falhas identificadas, dificuldades de comunicação, lacunas de documentação e oportunidades de melhoria na implementação das medidas de privacidade e de segurança da informação previstas no PPSI. Esse relatório é apresentado aos comitês envolvidos ou estrutura equivalente, subsidiando ajustes nos fluxos, procedimentos internos e ações do plano de trabalho do PPSI. Além disso, as lições aprendidas são incorporadas às ações de conscientização e às atualizações das políticas e normas internas pertinentes.

*Atribuição: As imagens ilustrativas associadas aos papéis foram desenhadas por Freepik.

gov.br

# Dúvida?

## Entre em contato conosco

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

**E-mail:**
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