gov.br

MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS

GOVERNO FEDERAL BRASIL UNIÃO E RECONSTRUÇÃO

Cartilha de Estruturação Básica de Gestão em Privacidade e Segurança da Informação

Programa de Privacidade e Segurança da Informação (PPSI)

Versão 1.0
Brasília, novembro de 2024

MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS

Esther Dweck

Ministra

SECRETARIA DE GOVERNO DIGITAL

Rogério Souza Mascarenhas

Secretário de Governo Digital

DIRETORIA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

Leonardo Rodrigo Ferreira

Diretor de Privacidade e Segurança da Informação

COORDENAÇÃO-GERAL DE PRIVACIDADE

Julierme Rodrigues da Silva

Coordenador-Geral de Privacidade

COORDENAÇÃO-GERAL DE SEGURANÇA DA INFORMAÇÃO

Loriza Andrade Vaz de Melo

Coordenadora-Geral de Segurança da Informação

Equipe Técnica de Elaboração

Anderson Souza de Araújo

Bruno Pierre Rodrigues de Sousa

Leonard Keyzo Yamaoka Batista

Rafael da Silva Ribeiro

Equipe Revisora

Adriano de Andrade Moura

Anderson Souza de Araújo

Rogério Vinícius Matos Rocha

CARTILHA SOBRE ESTRUTURAÇÃO BÁSICA DE GESTÃO EM PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

A **presente Cartilha**, especialmente recomendada e dirigida aos órgãos e às entidades da Administração Pública Federal - APF, visa auxiliar os órgãos na implementação de ações específicas de conformidade básica estabelecidas pela IN SGD/ME nº 94, de 23 de dezembro de 2022, pela IN CGU nº 3, de 9 de junho de 2017, pela IN GSI/PR nº 1, de 27 de maio de 2020 e pela Lei Geral de Proteção de Dados Pessoais - LGPD - Lei nº 13.709, de 14 de agosto de 2018.

Este documento é de autoria exclusiva da Secretaria de Governo Digital (SGD) do Ministério da Gestão e da Inovação em Serviços Públicos e tem como referência fundamental o Guia do Framework de Privacidade e Segurança da Informação, que é baseado em diversas publicações e documentos técnicos já existentes que são utilizados amplamente por profissionais da área de privacidade e segurança da informação.

Introdução

Esta cartilha tem como objetivo fornecer orientações ao órgão ou entidade, no cumprimento da sua missão institucional, para auxiliar na adoção das medidas que se referem a estruturação básica em Privacidade e Segurança da Informação (SI), bem como proporcionar elementos à alta administração e aos gestores das organizações da Administração Pública Federal (APF) direta, autárquica e fundacional, que desempenham papel fundamental na implementação das medidas propostas por este controle, especialmente, no que se refere a garantir que a estruturação básica seja efetivamente estabelecida no órgão ou entidade.

O Controle 0 (zero) do **Guia do Framework de Privacidade e Segurança da Informação**[1] (p. 103, 104 e 105) estabelece que:

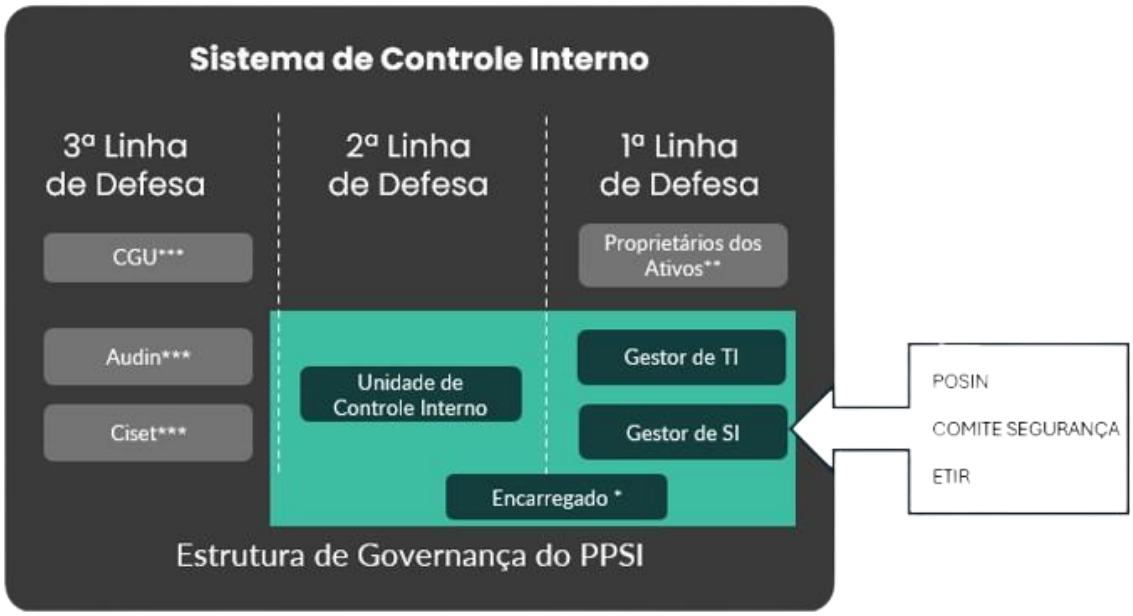
Controle 0: Estruturação básica de gestão em privacidade e segurança da Informação.

Essa **Cartilha** auxilia na adoção das medidas: **0.1, 0.2, 0.3, 0.4, 0.5, 0.6 e 0.7**.

[1] Acesse o Guia do Framework do PPSI em:
https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_framework_psi.pdf

Estrutura Básica de Gestão em Privacidade e Segurança da Informação

A estruturação básica tem fundamento na política de governança da APF direta, autárquica e fundacional (Decreto nº 9.203, de 22 de novembro de 2017), e contempla os seguintes papéis fundamentais para condução e implementação do Framework PPSI:



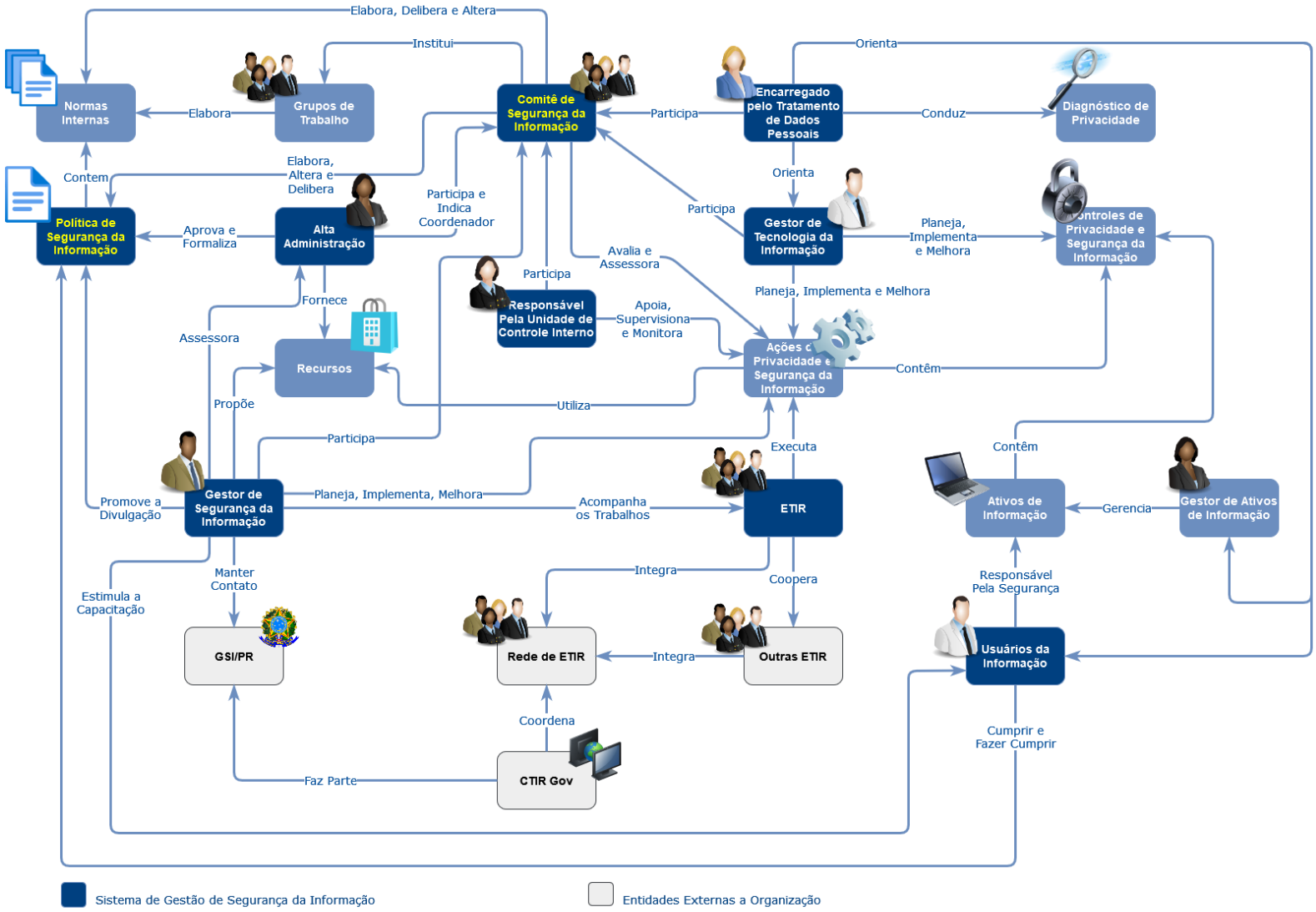
* O(A) Encarregado(a) compõe a Estrutura de Governança do PPSI e atuará com orientações e suporte nas questões que envolvem a Privacidade e Proteção de Dados Pessoais nas duas linhas de defesa (1ª e 2ª).

** Também compõe a primeira linha de defesa os gestores de negócios ou de políticas públicas envolvidas.

*** CGU, Audin e Ciset compõem a terceira linha de defesa, para mais informações acesse: Instrução Normativa nº 3, de 09 de junho de 2017

MAPA CONCEITUAL

Estrutura Básica de Gestão em Privacidade e Segurança da Informação



Fonte: https://www.escolavirtual.gov.br/trilha/246

Primeira Linha de Defesa

A primeira linha de defesa é responsável por identificar, avaliar, controlar e mitigar riscos, guiando o desenvolvimento e a implementação de políticas e procedimentos internos para garantir que as atividades estejam de acordo com as metas e objetivos da organização. Ela contempla os controles primários que devem ser instituídos e mantidos pelos gestores responsáveis pela implementação das políticas públicas durante a execução de atividades finalísticas e de apoio. Para garantir sua adequação e eficácia, os controles internos devem ser integrados ao processo de gestão, dimensionados e desenvolvidos na proporção requerida pelos riscos de acordo com a natureza, complexidade, estrutura e a missão da organização.[2]

[2] Saiba mais:
https://repositorio.cgu.gov.br/bitstream/1/33409/19/Instrucao_Normativa_CGU_3_2017.pdf

Gestor(a) de TI e Gestor(a) de Segurança da Informação[3]

Planeja, implementa e melhora as ações e controles de privacidade e SI, bem como orientar a equipe de TI para garantir que os Controles de Privacidade e SI sejam aplicados de forma eficaz. Participa do Comitê de SI e trabalha em cooperação com o(a) Encarregado(a)

Coordena e promove a divulgação da Política de SI e propõe melhorias. Mantém contato com a GSI/PR* e assessora a Alta Administração e outros na execução das políticas de segurança. Propõe recursos para as ações de privacidade e SI, planeja, implementa e melhora estas ações. Acompanha os trabalhos da ETIR.

Participa do Comitê de SI e orienta o(a) Gestor(a) de TI, os(as) Gestores(as) dos Ativos de Informação, o Comitê de SI e os Usuários da Informação na implementação dos Controles Privacidade e SI. Conduz a realização de diagnósticos de privacidade para garantir que as práticas de tratamento de dados pessoais estejam em compliance.

* GSI/PR: Gabinete de Segurança Institucional da Presidência da República

** O(A) Encarregado(a) atuará com orientações e suporte nas questões que envolvem a Privacidade e Proteção de Dados Pessoais nas duas linhas de defesa (1ª e 2ª).

[3] Instrução Normativa GSI/PR nº 1/2020

Política de Segurança da Informação[4]

Documento aprovado pela autoridade máxima responsável pelo órgão ou entidade da administração pública federal, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação.

O GSI em sua IN 01/2020[5] diz ser obrigatório a todos órgãos ou entidades da APF possuir uma Política de Segurança da Informação - POSIN.

A POSIN deve ser elaborada sob a coordenação do **Gestor de Segurança da Informação com a participação do Comitê de Segurança da Informação Interno ou estrutura equivalente**.

A **autoridade máxima** do órgão ou da entidade é responsável por garantir os recursos necessários para a execução da POSIN no âmbito de sua organização.

Estrutura Mínima da POSIN

- Escopo;
- Conceitos e Definições;
- Princípios;
- Diretrizes Gerais:
  - Tratamento da Informação;
  - Segurança Física e do Ambiente;
  - Gestão de Incidentes;
  - Gestão de Ativos
  - Gestão de uso de recursos operacionais e de comunic.;
  - Controles de Acesso;
  - Gestão de Riscos;
  - Gestão de Continuidade;
  - Auditoria e Conformidade;
- Competências;
- Penalidades;
- Política de atualização (< 4 anos)

[4] Modelo de POSIN: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/modelo_politica_seguranca_informacao.docx

[5] Saiba mais em: Instrução Normativa GSI/PR nº 1/2020

Comitê de Segurança da Informação

Grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação no âmbito do órgão ou entidade da administração pública federal.

Composição[6]

- Gestor de Segurança da Informação do órgão ou da entidade;[7]
- Um representante da Secretaria-Executiva ou da **unidade equivalente** do órgão ou da entidade;

- Um representante de cada unidade finalística do órgão ou da entidade;
- O titular da unidade de tecnologia da informação do órgão ou da entidade.
O Comitê de Segurança da Informação será coordenado pela maior autoridade designada.

Atribuições

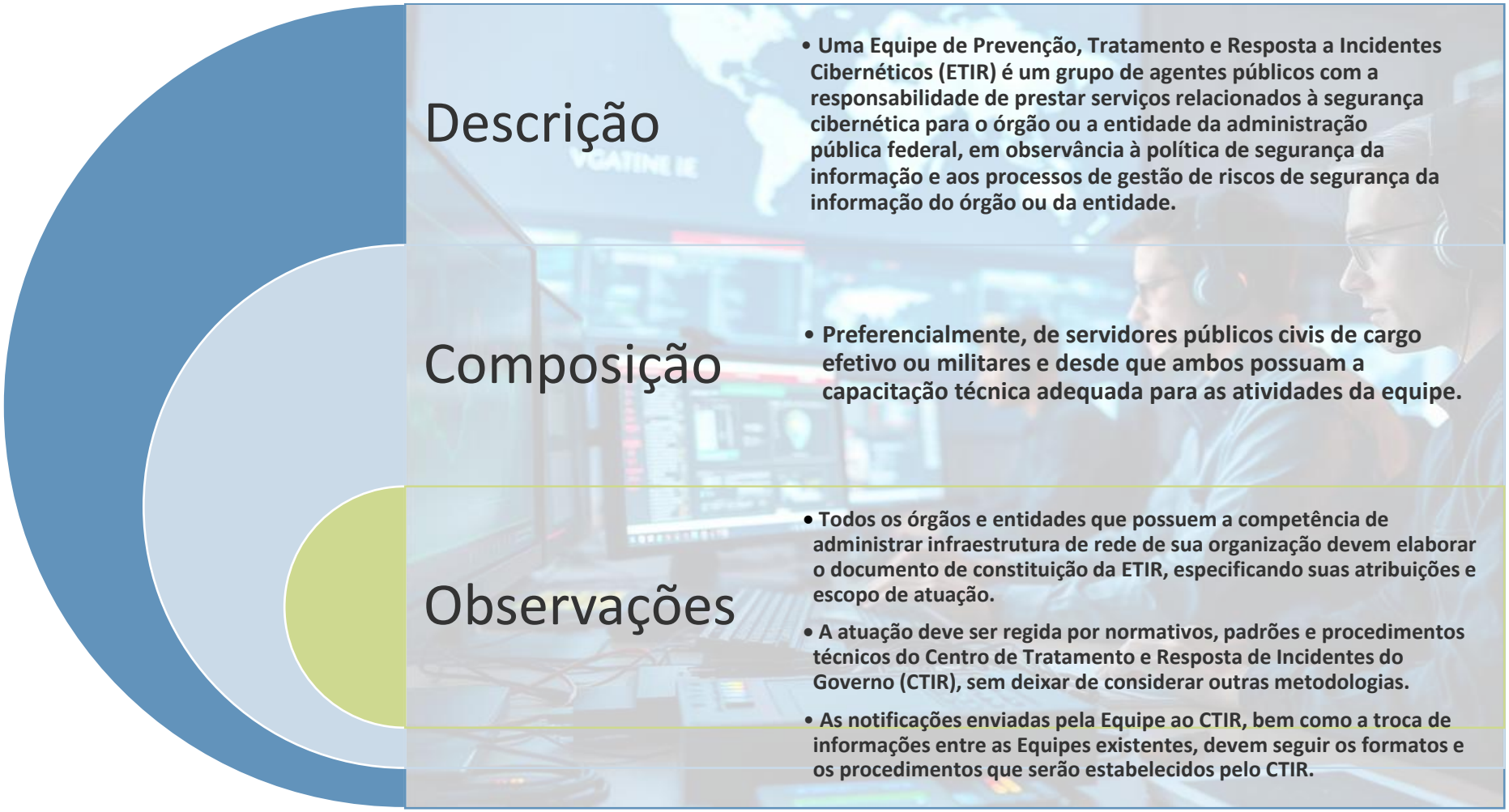
- assessorar a implementação das ações de segurança da informação.
- constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação.
- participar da elaboração da Política de Segurança da Informação e das normas internas de segurança da informação.
- propor alterações à Política de Segurança da Informação e às normas internas de segurança da informação.
- deliberar sobre normas internas de segurança da informação.
- 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.

---

[6] Instrução Normativa GSI/PR nº 01/2020

[7] Instrução Normativa GSI/PR n° 07/2022

Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR)[8]



[8] Fonte: Instrução Normativa GSI/PR nº 01/2020

Segunda Linha de Defesa

A segunda linha de defesa[9] objetiva assegurar que as atividades realizadas pela primeira linha sejam desenvolvidas e executadas de forma apropriada. Assim, as instâncias da segunda linha de defesa, situadas ao nível da gestão, são destinadas a apoiar o desenvolvimento dos controles internos da gestão e realizar atividades de supervisão e de monitoramento das atividades desenvolvidas no âmbito da primeira linha de defesa, que incluem gerenciamento de riscos, conformidade, verificação de qualidade, controle financeiro, orientação e treinamento. Os Assessores e Assessorias Especiais de Controle Interno (AECI) nos Ministérios integram a segunda linha de defesa e podem ter sua atuação complementada por outras estruturas específicas definidas pelas próprias organizações.

[9] Saiba mais em: https://repositorio.cgu.gov.br/bitstream/1/33409/19/Instrucao_Normativa_CGU_3_2017.pdf

Responsável pela Unidade de Controle[10] Interno e Encarregado(a)[11]

Atuará no apoio, supervisão e monitoramento das atividades desenvolvidas pela primeira linha de defesa prevista pela Instrução Normativa CGU nº 3, de 9 de junho de 2017.
Devem assegurar que as atividades realizadas pela primeira linha sejam desenvolvidas e executadas de forma apropriada. Apoiar o desenvolvimento dos controles internos da gestão.

Participa do Comitê de Segurança da Informação e orienta o(a) Gestor(a) de Tecnologia da Informação, os(as) Gestores(as) dos Ativos de Informação, o Comitê e os Usuários da Informação na implementação dos Controles Privacidade e Segurança da Informação. Também conduz a realização de diagnósticos de privacidade para garantir que as práticas de tratamento de dados pessoais estejam em conformidade com a legislação vigente.

* O(A) Encarregado(a) atuará com orientações e suporte nas questões que envolvem a Privacidade e Proteção de Dados Pessoais nas duas linhas de defesa (1ª e 2ª).

[10] Fonte: Instrução Normativa CGU nº 3, de 9 de junho de 2017

[11] Saiba mais em: ANPD – Guia Orientativo: Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado

Diretoria de Privacidade e Segurança da Informação

Secretaria de Governo Digital (SGD/MGI)

Coordenação-Geral de Privacidade (CGPRI/DPSI/SGD/MGI)

E-mail: ppsi.sgd@gestao.gov.br

Governo Digital > Privacidade e Segurança

https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca