Programa de Privacidade e Segurança da Informação (PPSI)

Secretaria de Governo Digital

Novembro de 2022

Framework de Privacidade e Segurança da Informação
Agenda

1. **O PPSI e a Motivação do Framework**
2. **Estruturação do Guia do Framework**
3. **Ferramenta de Automação do Framework**

O PPSI e Motivação do Framework

Framework de Privacidade e Segurança da Informação

OBJETIVO

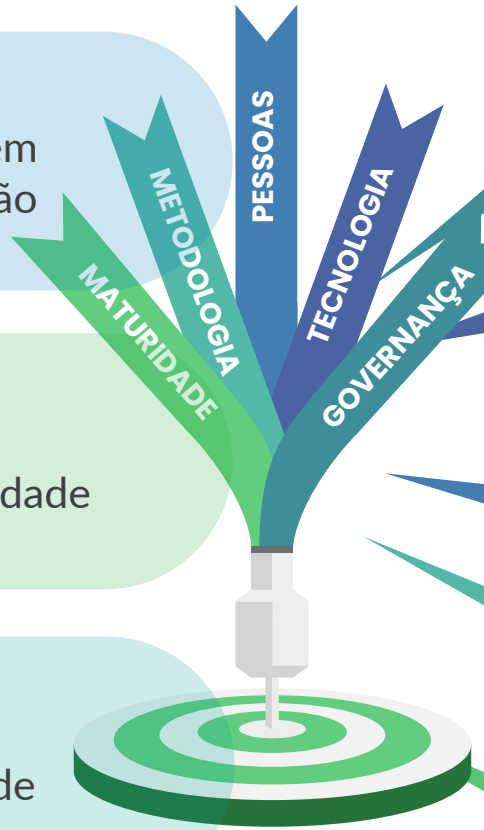
Elevar a maturidade e resiliência em privacidade e segurança da informação dos órgãos do SISP

RESULTADO-CHAVE 1

Implementação de controles de privacidade

RESULTADO-CHAVE 2

Implementação de controles de segurança da informação



Principais iniciativas de apoio

- Centro Integrado de Segurança Cibernética do Governo Digital – CISC GOV.BR
- Pentest e Simulação de Phishing
- Centro de Excelência em Privacidade e Cibersegurança (PCCoE)
- Framework de Privacidade e Segurança da Informação (LGPD, PNSI)
- Control Self Assessment (CSA), Análise de GAPs, Plano Trabalho e Monitoramento

Framework de Privacidade e Segurança da Informação
Motivação

Decreto 10.332/2020
EGD 2020-2022

Objetivo 10 - Implementação da LGPD no âmbito do Governo federal

Objetivo 11 - Garantia da segurança das plataformas de governo digital e de missão crítica

Acórdãos TCU

Acórdão 1889/2020
Sistemas Informacionais Críticos

Acórdão 1384/2022*
Diagnóstico do Grau de Implementação da LGPD na APF

Acórdão 1768/2022
Mapeamento Maturidade APF quanto à Implementação de Controles Críticos de SEGCIBER

* 9.1. recomendar à SGD/ME (...) que considerando o controle sob jurisdição, edite normativos e guias, **consultando ANPD** e GSI/PR, **para auxiliar a adequação das organizações à LGPD**.

Estruturação do Guia do Framework

Framework de Privacidade e Segurança da Informação
Guia

1

OBJETIVO

Propor às instituições públicas diretrizes no sentido de auxiliar a identificação, o acompanhamento e o preenchimento das lacunas de privacidade e segurança da informação presentes na instituição com base nos controles elaborados pelo(a) CIS, NIST, ISO/IEC e ABNT NBR.

2

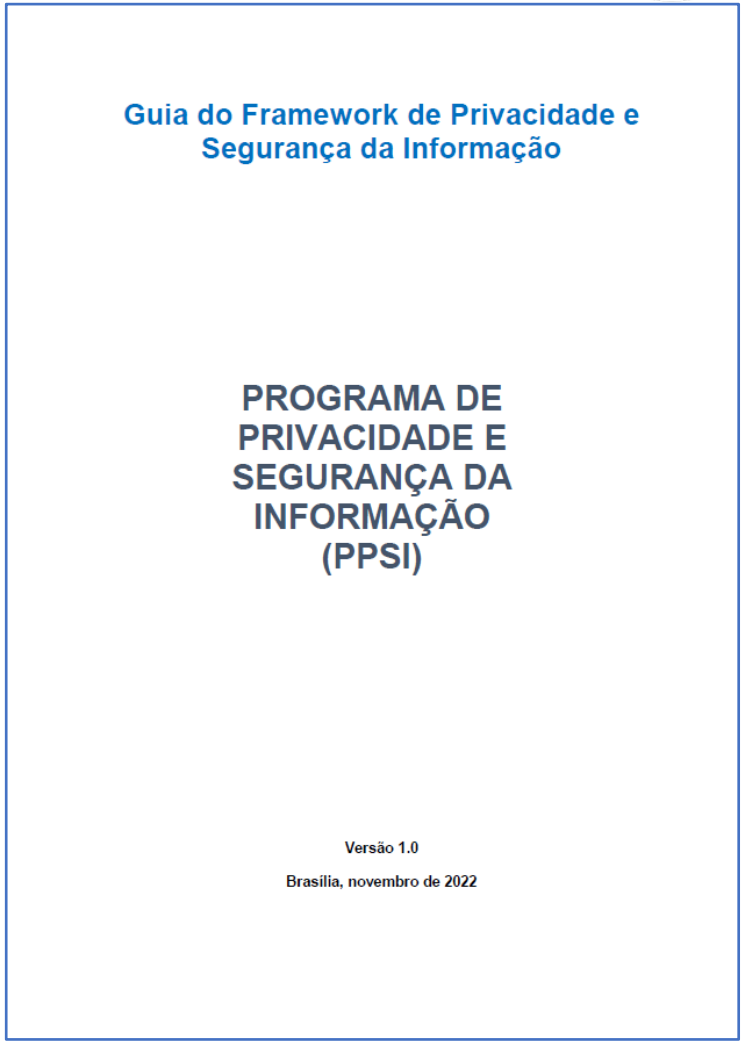
ELABORAÇÃO

Ação conduzida pelas Torres de Metodologia e Maturidade do Departamento de Privacidade e Segurança da Informação.

3

ORGANIZAÇÃO DO GUIA

Guia do Framework estruturado em 8 Capítulos e 5 Anexos.



Framework de Privacidade e Segurança da Informação
Estruturação do Guia - Capítulos

O **Guia do Framework** foi estruturado em 8 capítulos:

1. FUNDAMENTAÇÃO
2. CONTROLE DE ESTRUTURAÇÃO BÁSICA EM SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE
3. CONTROLES DE CIBERSEGURANÇA
4. CONTROLES DE PRIVACIDADE
5. IMPLEMENTAÇÃO
6. MATURIDADE
7. FERRAMENTA DE ACOMPANHAMENTO DA IMPLEMENTAÇÃO DO FRAMEWORK
8. CONSIDERAÇÕES FINAIS

Capítulo 1 - Fundamentação

"Não há privacidade sem segurança"

1. Normas legais de conformidade

- LGPD
- Normativos GSI
- PNSI – Política Nacional de Segurança da Informação

2. Estruturação básica de gestão em privacidade e segurança

- Dirigente de TI
- Gestor de Segurança da Informação
- Responsável pela Unidade de Controle Interno
- Comitê de Segurança da Informação ou equivalente
- Equipe de Tratamento e Resposta a Incidentes Cibernéticos – ETIR
- Encarregado pela Proteção de Dados Pessoais
- Política de Segurança da Informação

3. Abordagem de controles e implementação de cibersegurança

- CIS Controls – Cibersegurança
- CIS Guia Complementar de Privacidade
- Grupos de Implementação do CIS
- NIST Cybersecurity Framework (Identificar-Proteger-Detectar-Responder- Recuperar)

4. Abordagem de controles e implementação de privacidade

- ISO/IEC 29100:2011
- ISO/IEC 29151:2017
- ABNT NBR ISO/IEC 27701:2019
- ISO/IEC 27018:2014
- ISO/IEC 29134:2017
- ABNT NBR ISO/IEC 29184:2021
- NIST Privacy Framework (Identificar, Governar, Controlar, Comunicar, Proteger)
- Guias Orientativos da ANPD

Capítulo 2 – Estruturação básica em privacidade e segurança da informação

Capítulo 2

Referências Normativas

IN SGD/ME nº 01/2019

IN CGU nº 3/2017

IN GSI/PR nº 1/2020

Lei nº 13.709/2018 (LGPD)

Responsabilidade da Alta Administração

Garantir que estruturação básica em segurança da informação e privacidade seja estabelecida no órgão ou entidade.

Capítulo 2

Conformidade básica relativa aos atores essenciais para condução do Framework

Anexo III

Controle 0

- Dirigente TI
- Gestor de Segurança da Informação
- Responsável pela Unidade de Controle Interno
- Comitê de Segurança da Informação ou equivalente
- ETIR
- Encarregado
- POSIN

Anexo III – Controle de estruturação básica em segurança da informação e privacidade

CONTROLE 0: ESTRUTURAÇÃO BÁSICA DE GESTÃO EM PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

ID	FUNÇÃO NIST CSF	MEDIDA	REFERÊNCIAS
0.1	------	O órgão nomeou uma autoridade máxima de Tecnologia da Informação?	Instrução Normativa SGD/ME nº 01, de 4 de abril de 2019
0.2	------	O órgão nomeou um Gestor de Segurança da Informação?	Art. 15, inciso I da Instrução Normativa GSI nº 1, de 27 de maio de 2020
0.3	------	O órgão nomeou um responsável pela unidade de controle interno?	Instrução Normativa CGU nº 3, de 9 de junho de 2017
0.4	------	O órgão instituiu um Comitê de Segurança da Informação?	Art. 15, inciso II da Instrução Normativa GSI Nº 1 - 27 de maio de 2020
0.5	------	O órgão instituiu uma Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR?	Art. 15, inciso IV da Instrução Normativa GSI Nº 1 - 27 de maio de 2020
0.6	------	O órgão elaborou uma Política de Segurança da Informação - POSIN?	Art. 9º da Instrução Normativa GSI Nº 1 - 27 de maio de 2020
0.7	GOVERNAR-P	O órgão nomeou um Encarregado pelo Tratamento de Dados Pessoais?	Art. 41 da Lei Geral de Proteção de Dados Pessoais, de 14 de agosto de 2018

Capítulo 3 - Controles de Cibersegurança (CIS 8)

Controles CIS 8

- 01: INVENTÁRIO E CONTROLE DE ATIVOS INSTITUCIONAIS
- 02: INVENTÁRIO E CONTROLE DE ATIVOS DE SOFTWARE
- 03: PROTEÇÃO DE DADOS
- 04: CONFIGURAÇÃO SEGURA DE ATIVOS INSTITUCIONAIS E SOFTWARE
- 05: GESTÃO DE CONTAS
- 06: GESTÃO DO CONTROLE DE ACESSO
- 07: GESTÃO CONTÍNUA DE VULNERABILIDADES
- 08: GESTÃO DE REGISTROS DE AUDITORIA
- 09: PROTEÇÕES DE E-MAIL E NAVEGADOR WEB
- 10: DEFESAS CONTRA MALWARE
- 11: RECUPERAÇÃO DE DADOS
- 12: GESTÃO DA INFRAESTRUTURA DE REDE
- 13: MONITORAMENTO E DEFESA DA REDE
- 14: CONSCIENTIZAÇÃO E TREINAMENTO DE COMPETÊNCIAS SOBRE SEGURANÇA
- 15: GESTÃO DE PROVEDOR DE SERVIÇOS
- 16: SEGURANÇA DE APLICAÇÕES
- 17: GESTÃO DE RESPOSTA A INCIDENTES
- 18: TESTES DE INVASÃO

Capítulo 3

- Contextualização do objetivo do controle
- Por que implementar?
- Aplicabilidade e Implicações de Privacidade
- Fique Atento!

Anexo IV

Controles 1 a 18

- Medidas de Cibersegurnaça a serem implementadas para os controles.

3.1 Controle 1: Inventário e Controle de Ativos Institucionais

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

Por que implementar?

As instituições não podem defender aquilo que não está mapeado ou não se tem conhecimento de sua existência. Por esta razão, ter um inventário de ativos institucionais é essencial para que uma atitude de defesa possa acontecer.

3.1.1 Aplicabilidade e Implicações de Privacidade

Princípios de privacidade devem ser incorporados ao processo de inventário de dispositivos, tanto do ponto de vista tecnológico quanto do processual. O conhecimento sobre um dispositivo, onde está localizado, quem o está usando e como o está usando pode fornecer dados pessoais, muitas instituições usam o nome ou identificador de um indivíduo, que o vincula explicitamente ao dispositivo.

Fique Atento!

A Secretaria de Governo Digital disponibiliza em seu portal um Modelo de Política de Gestão de Ativos, com enfoque em prover diretrizes para gestão de ativos que constitui referência importante para instituições e profissionais de segurança da informação, que desejam realizar o gerenciamento de ativos da instituição.

Disponível em: Modelo de Política de Gestão de Ativos da SGD

Anexo IV – Tabela de Medidas e Controles de Cibersegurança

CIBERSEGURANÇA CONTROLE 1: INVENTÁRIO E CONTROLE DE ATIVOS INSTITUCIONAIS

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMEN-TAÇÃO
1.1	1.1	IDENTIFICAR	O órgão estabelece e mantém um inventário detalhado de ativos institucionais?	Estabelecer e manter um inventário preciso, detalhado e atualizado de todos os ativos institucionais com potencial para armazenar ou processar dado. Certificar de que o inventário registrará o endereço de rede (se estático), endereço de hardware, nome da máquina, etc. Deverá incluir ativos conectados à infraestrutura física, virtual, e remota e aqueles dentro de ambientes de nuvem. Necessário incluir também ativos mesmo que não estejam sob controle do órgão. Revisar e atualizar o inventário semestralmente ou com mais frequência.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 1/2020 IN nº 3/2021 IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 12 /IN01/.DSIC/GSIPR	1, 2, 3
1.2	1.4	IDENTIFICAR	O órgão usa o Dynamic Host Configuration Protocol DHCP para Atualizar o Inventários de Ativos?	Utilizar o registro (logs) do Dynamic Host Configuration Protocol (DHCP) em todos os servidores DHCP ou utilizar uma ferramenta de gerenciamento de endereços IP para atualizar o inventário de ativos de hardware da instituição.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	NC 08 /IN01/DSIC/GSIPR	2, 3
1.3	1.3	DETECTAR	O órgão usa uma ferramenta de descoberta ativa?	Identificar ativos conectados à rede institucional através de uma ferramenta de descoberta ativa. Configurar para que essa descoberta seja executada diariamente ou com mais frequência.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	NC 08 /IN01/DSIC/GSIPR	2, 3
1.4	1.5	DETECTAR	O órgão usa ferramenta de Descoberta Passiva?	Utilizar uma ferramenta de descoberta passiva para identificar dispositivos conectados à rede da instituição e automaticamente atualizar o inventário de ativos de hardware da instituição.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR	3

Capítulo 4 - Controles de Privacidade

Controles de Privacidade

- 19: INVENTÁRIO E MAPEAMENTO
- 20: FINALIDADE E HIPÓTESES LEGAIS
- 21: GOVERNANÇA
- 22: POLÍTICAS, PROCESSOS E PROCEDIMENTOS
- 23: CONSCIENTIZAÇÃO E TREINAMENTO
- 24: MINIMIZAÇÃO DE DADOS
- 25: GESTÃO DO TRATAMENTO
- 26: ACESSO E QUALIDADE
- 27: COMPARTILHAMENTO, TRANSFERÊNCIA E DIVULGAÇÃO
- 28: SUPERVISÃO EM TERCEIROS
- 29: ABERTURA, TRANSPARÊNCIA E NOTIFICAÇÃO
- 30: AVALIAÇÃO DE IMPACTO, MONITORAMENTO E AUDITORIA
- 31: SEGURANÇA APLICADA A PRIVACIDADE

Capítulo 4

- Contextualização do objetivo do controle
- Por que implementar?
- Fique Atento!

Anexo V

Controles 19 a 31

- Medidas de privacidade a serem implementadas para os controles.

4.1 Controle 19: Inventário e Mapeamento

As operações de tratamento de dados pessoais por sistemas, produtos, processos ou serviços devem ser identificadas e inventariadas.

Por que implementar?

De acordo com o Art. 37 da LGPD o controlador e o operador devem manter registradas as operações de tratamento de dados pessoais que realizam, especialmente quando baseadas no legítimo interesse.

O Registro de Operações de tratamento de dados pessoais representa uma operação importante de governança de dados pessoais e de subsídio para avaliação de impacto à proteção de dados pessoais com vistas a verificar a conformidade da instituição no que se refere ao preconizado pela LGPD.

Uma maneira de manter os registros de tratamento de dados pessoais é manter um inventário ou uma lista das atividades de tratamento que a organização realiza.

Fique Atento!

A Secretaria de Governo Digital disponibiliza em seu portal um Guia de Inventário de Dados Pessoais, que incentiva a adoção de registros das operações de tratamento de dados pessoais e suas respectivas avaliações, sob a ótica dos princípios da LGPD e contém importantes instruções para que as instituições e seus colaboradores possam elaborar um inventário de dados pessoais.

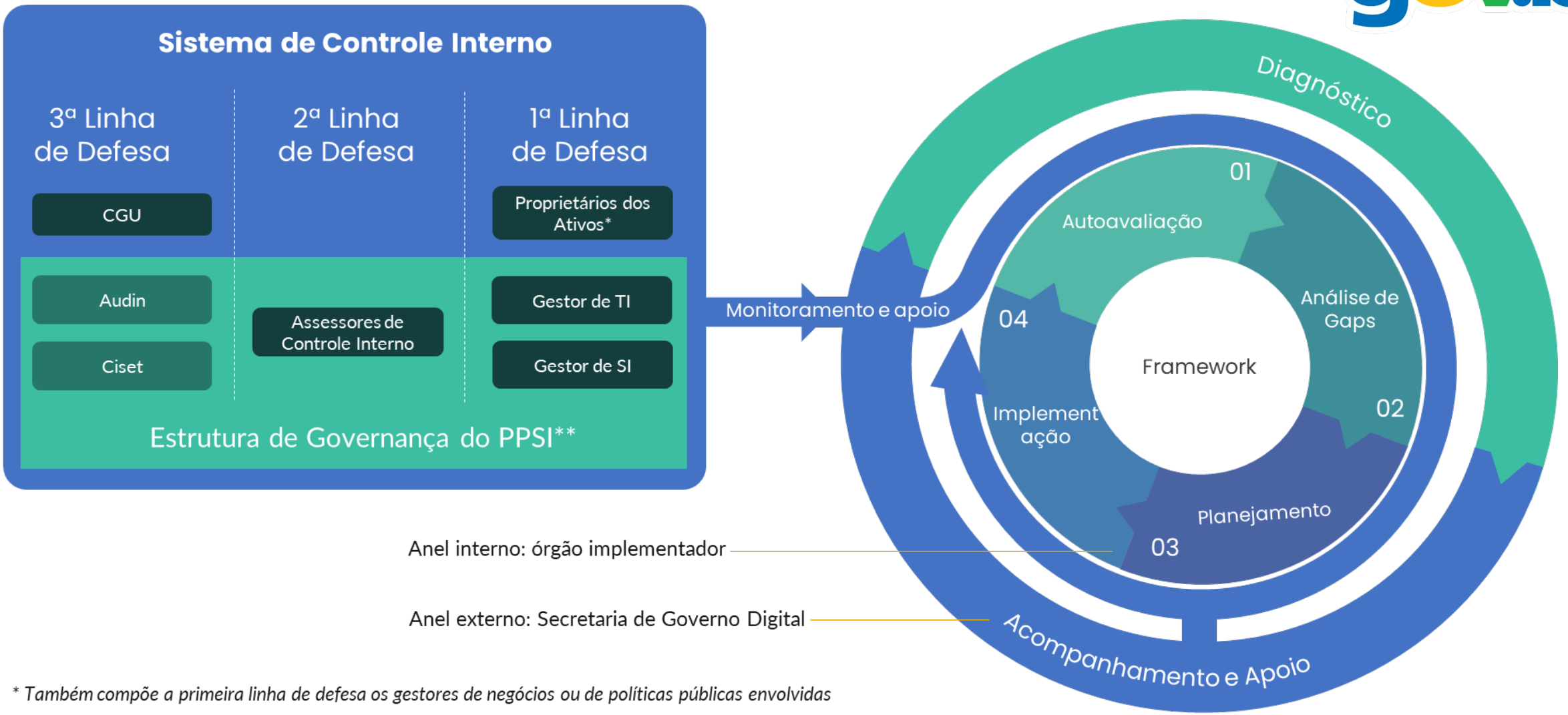
Disponível em: Guia de Elaboração de Inventário de Dados Pessoais da SGD

Anexo V – Tabela de Medidas e Controles de Privacidade

PRIVACIDADE CONTROLE 19: INVENTÁRIO E MAPEAMENTO

ID	FUNÇÃO NIST PF	DESCRIÇÃO DA MEDIDA	LGPD	REFERÊNCIAS ISO	NIST - PF
19.1	IDENTIFICAR-P	A organização documenta os sistemas, serviços e processos que tratam dados pessoais?	Art. 37	ABNT NBR ISO/IEC 27701:2019 (item 7.2.8)	NIST ID.IM-P1
19.2	IDENTIFICAR-P	O órgão mapeia os agentes de tratamento (controlador, co-controladores e operadores) responsáveis pelo processamento de dados pessoais?	Art. 37	ABNT NBR ISO/IEC 27701:2019 (item 7.2.8) ABNT NBR ISO/IEC 27701:2019 (item 7.2.7) ABNT NBR ISO/IEC 27701:2019, (itens 5.2.2)	NIST ID.IM-P2
19.3	IDENTIFICAR-P	O órgão documenta as fases do tratamento em que o operador atua?	Art. 16 Art. 37	ABNT NBR ISO/IEC 27701:2019 (item 7.2.1) ABNT NBR ISO/IEC 27701:2019 (item 7.2.8)	NIST ID.IM-P4 NIST CT.PO-P4
19.4	IDENTIFICAR-P	O órgão mapeia os fluxos ou ações do tratamento de dados pessoais?	Art. 37	ABNT NBR ISO/IEC 27701:2019 (item 7.2.8)	NIST ID.IM-P8
19.5	IDENTIFICAR-P	O órgão mapea o escopo (abrangência ou área geográfica) dos tratamentos de dados pessoais?	Art. 37	ABNT NBR ISO/IEC 27701:2019 (item 7.2.8)	N/A

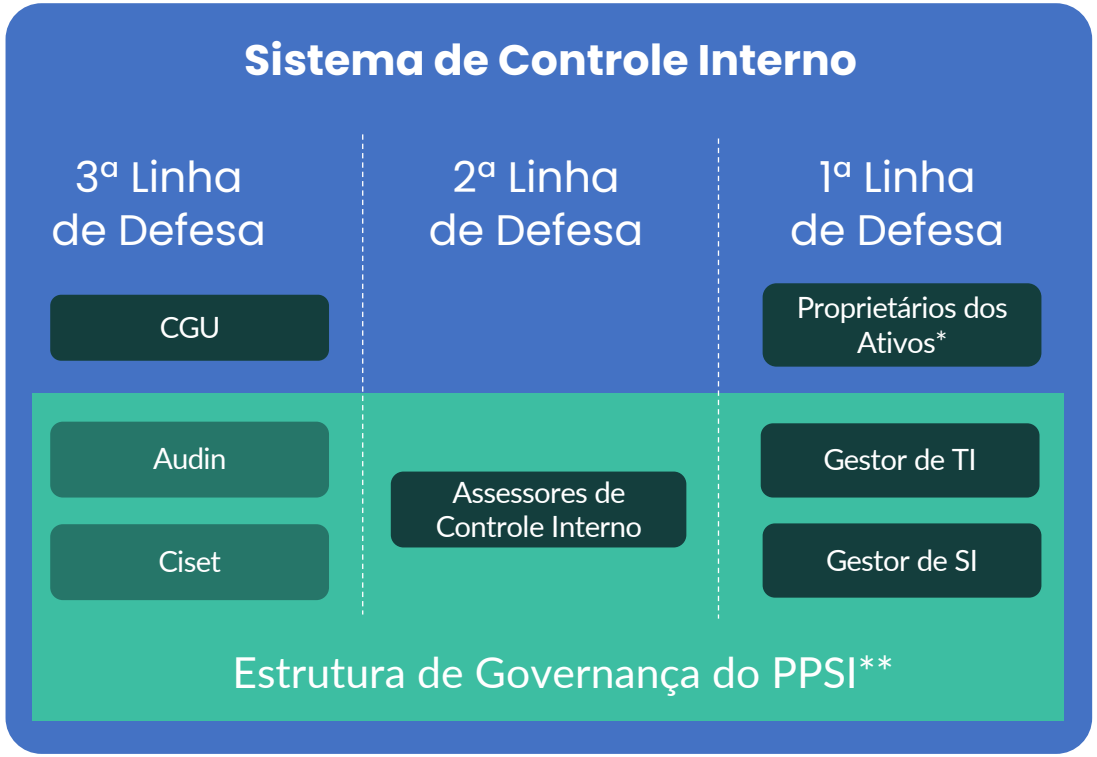
Capítulo 5 - Implementação



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

*** O Encarregado compõe a Estrutura de Governança do PPSI e atuará com orientações e suporte nas questões que envolvem a Privacidade e Proteção de Dados Pessoais*

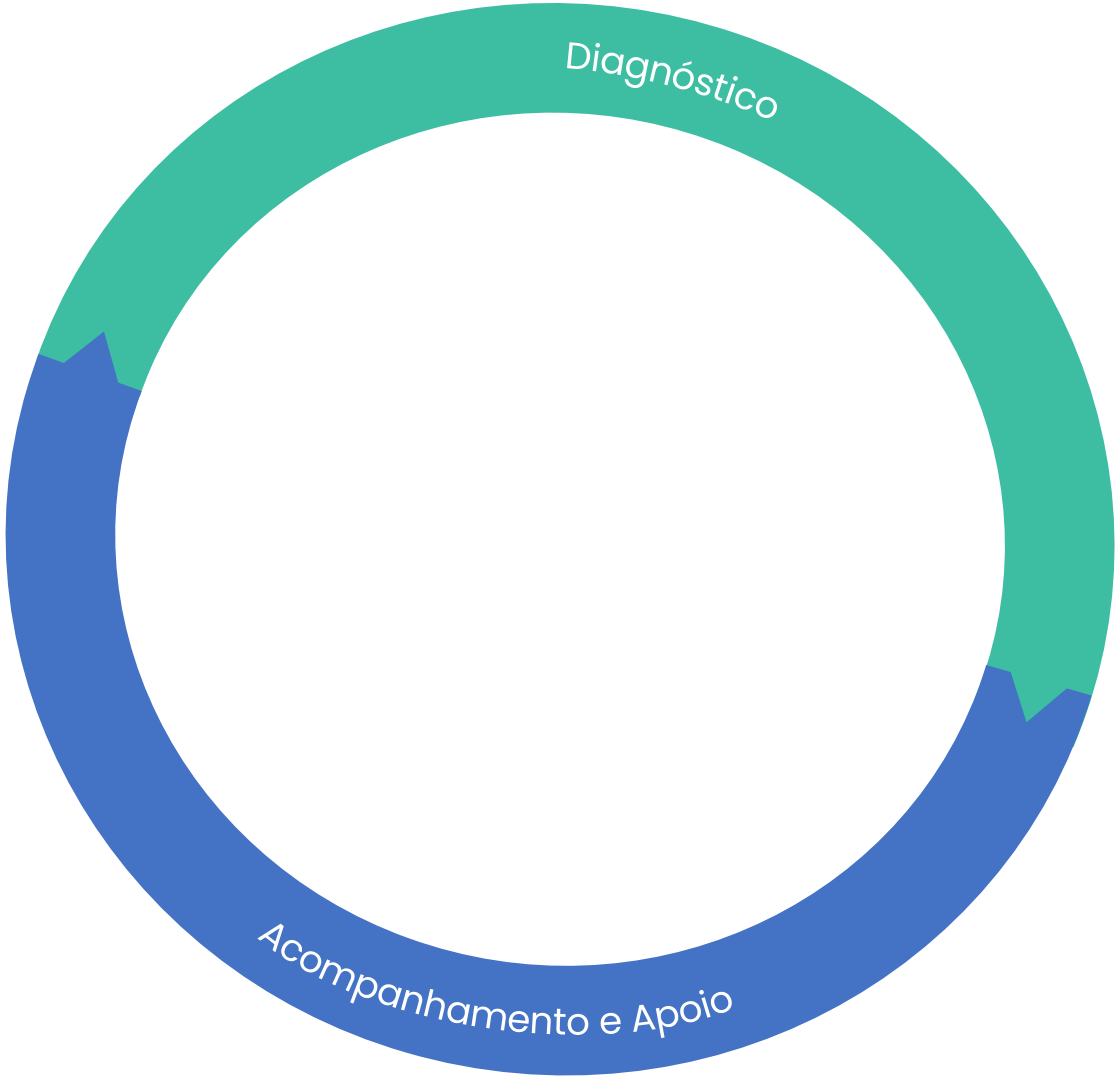
Capítulo 5 – Implementação
Sistema de Controle Interno



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

*** O Encarregado compõe a Estrutura de Governança do PPSI e atuará com orientações e suporte nas questões que envolvem a Privacidade e Proteção de Dados Pessoais*

Capítulo 5 – Implementação
Ciclo Externo



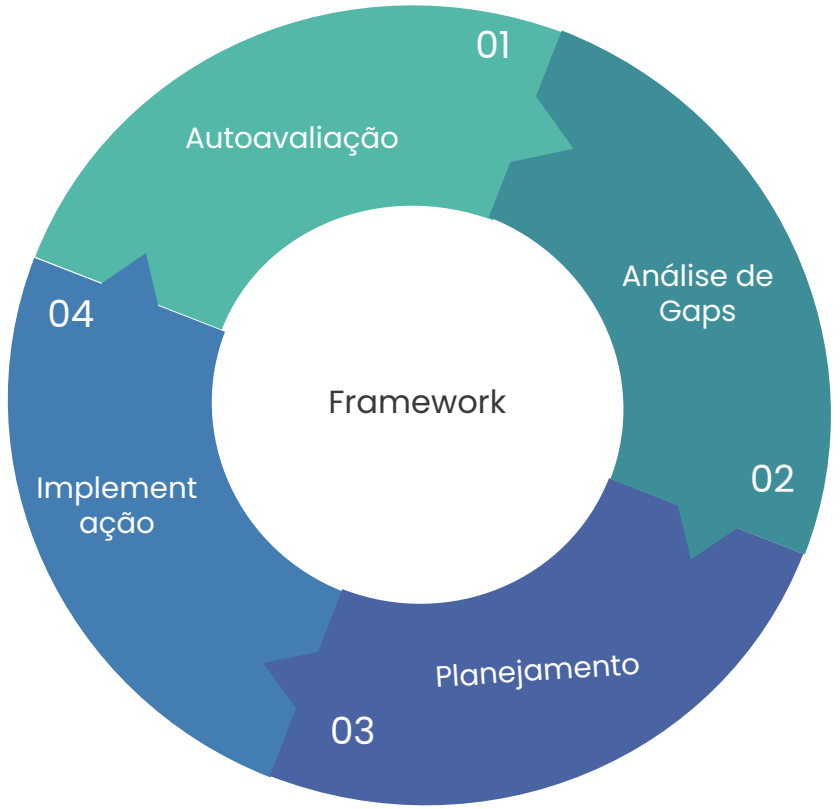
✓ Executado pelo **Departamento de Segurança da Informação e Privacidade** (**DPSI/SGD**).

✓ **Ações:**

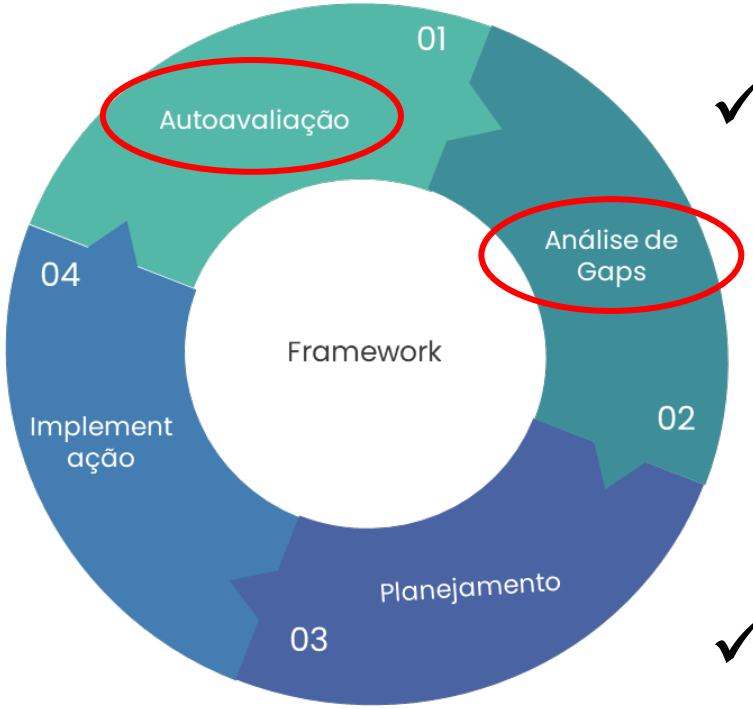
- Diagnóstico
  - Visão do nível de maturidade dos órgãos
- Acompanhamento e Apoio
  - Acompanhar implementação do plano de ação e fornecer apoio com reuniões técnicas e materiais para auxiliar a implementação do Framework.

Capítulo 5 – Implementação
Ciclo Interno

- ✓ É composto por etapas a serem executadas pelo órgão ou entidade implementador(a).
- ✓ Inspirado no modelo PDCA



Capítulo 5 - Implementação
Ciclo Interno

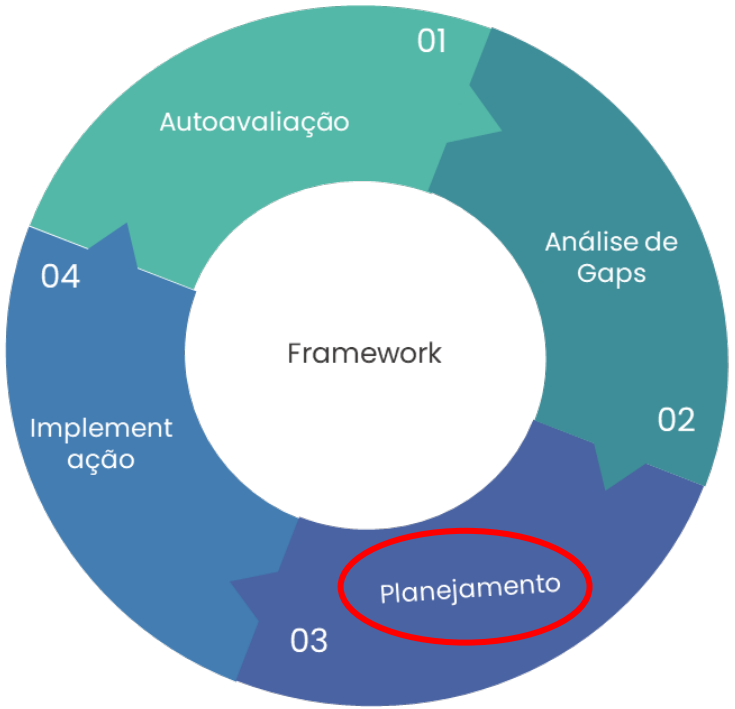


✓A autoavaliação terá como finalidade o autoconhecimento do órgão acerca dos controles e medidas adotadas em segurança cibernética e privacidade.

- Control Self-Assessment (CSA)

✓A análise de gaps consiste em identificar quais as falhas, lacunas ou melhorias relacionadas com privacidade e segurança da informação que foram identificadas na autoavaliação.

Capítulo 5 - Implementação
Ciclo Interno



- ✓ Estabelecer um plano de ação com as medidas de privacidade e segurança a serem implementadas ou aperfeiçoadas.
- ✓ Recomenda-se **priorizar o Controle 0**, as **medidas do GI1 do CIS** que tratam a higiene cibernética.

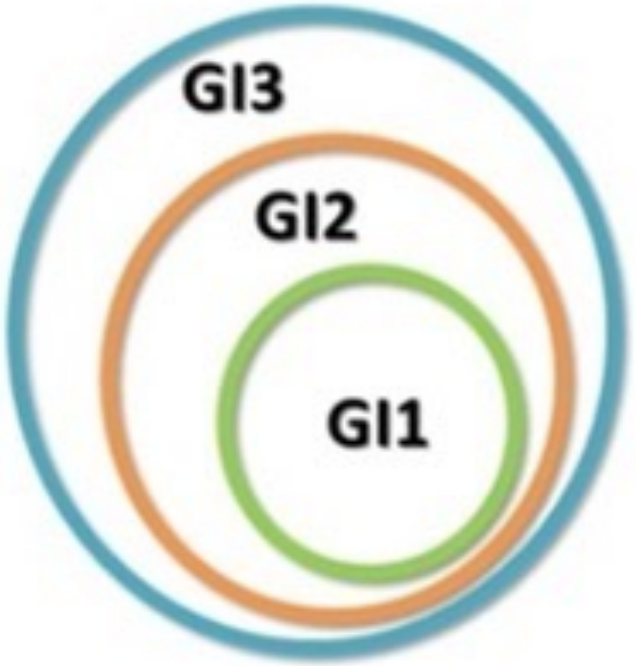
Grupo de Implementação do CIS (GI)	Framework - Aplicação das medidas
GI1 (IG1)	Aplicável para todas as instituições e seus ambientes tecnológicos independente da **complexidade do(s) sistema(s)***
GI1 (IG1) + GI2 (IG2)	Aplicável para ambientes tecnológicos que sustentam sistema(s) relevante(s) de **baixa e média criticidade***
GI1 (IG1) + GI2 (IG2) + GI3 (IG3)	Aplicável para ambientes tecnológicos que sustentam sistema(s) relevante(s) de **alta criticidade***

* O modelo de avaliação de complexidade de sistemas está descrito no Anexo I

A abordagem adotada por este Framework para **a escolha das medidas que constarão no GI1 de privacidade se baseia nas obrigações dispostas na LGPD**. A priorização das medidas de privacidade para o GI1 neste Framework se baseou **também, de forma complementar, na adoção das funções "Identificar-P" e "Governar-P" sugeridas pelo NIST Privacy Framework** como método simplificado para criar ou aprimorar um programa de privacidade.

Capítulo 5 - Implementação
Distribuição das Medidas nos Grupos de Implementação

GRUPOS DE IMPLEMENTAÇÃO



GI3 Sistema(s) relevante(s) de alta criticidade.

Segurança: 56 + 74 + 23 = 153 medidas
Privacidade: 97 + 37 + 16 = 150 medidas

GI2 Sistema(s) relevante(s) de baixa e média criticidade.

Segurança: 56 + 74 = 130 medidas
Privacidade: 97 + 37 = 134 medidas

GI1 Higiene cibernética - Independe da complexidade dos sistemas.

Segurança: 56 medidas
Privacidade: 97 medidas

Anexo I – Modelo de Avaliação de Criticidade de Sistemas

Identificar rol de sistemas → Selecionar sistema relevante

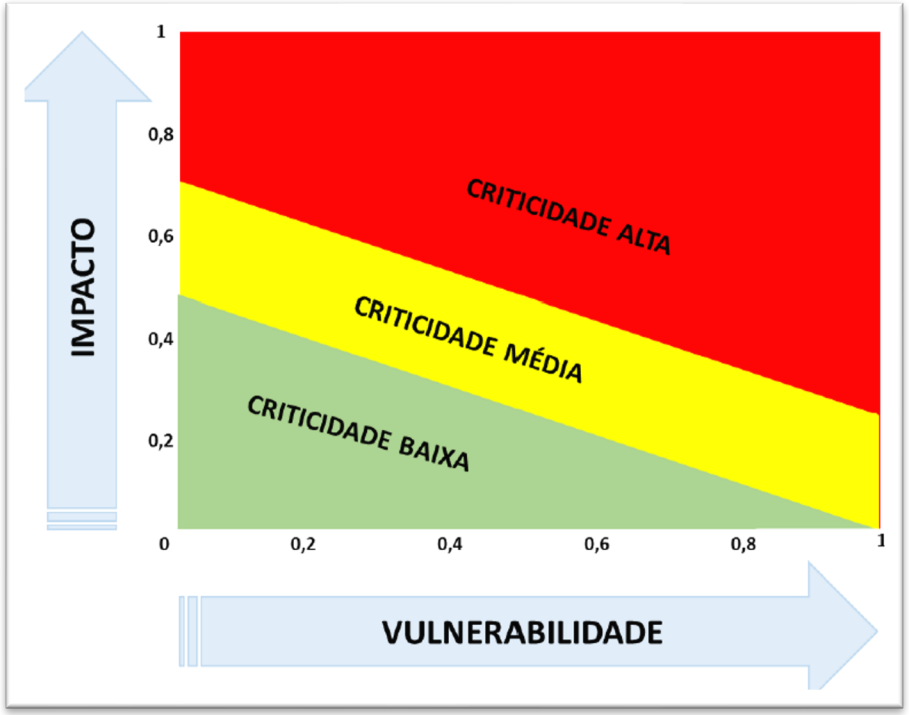
Avaliar eventuais **impactos** associados ao sistema relevante

+

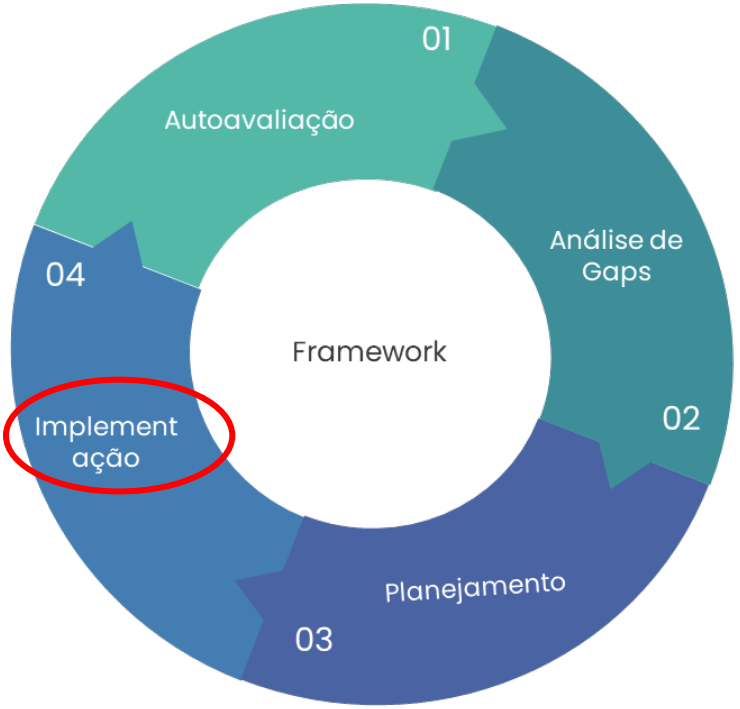
Avaliar eventuais **vulnerabilidades** associadas ao sistema relevante

→ Nota de criticidade

Acórdão 1889/2020-TCU-Plenário
identificar os sistemas informacionais críticos da APF



Capítulo 5 - Implementação
Ciclo Interno



✓Implementar os processos (controles e medidas) determinados na etapa anterior.

✓Considerar:

- Conscientização e Treinamento dos Implementadores;
- Monitoramento das Implementações;
  - Documentar dificuldades e progressos.
- Testes exaustivos dos controles e medidas implementados;
  - Aumento de confiabilidade do sistema.
- Ciclo de melhoria contínua.

Capítulo 6 - Maturidade

Premissa | *Metodologia enxuta para facilitar a avaliação dos órgãos e o acompanhamento pela SGD*

Níveis de Implementação

Avaliação por Medida

- Adota em maior parte ou totalmente
- Adota em menor parte
- Adota parcialmente
- Há decisão formal ou plano aprovado para implementar
- A organização não adota essa medida
- Não se aplica

Cálculo da Maturidade

Capítulo 6 – Maturidade
Abordagem em Profundidade

Control Self-Assessment (CSA)

Implementação

- Expressa uma análise sobre a amplitude de implementação da respectiva medida, considerando a abrangência de ativos de informação que possuem aplicabilidade
- Avaliação por **medida**
- 6 níveis de implementação

Capacidade

- Tem como objetivo avaliar o nível de efetividade da adequação de um controle
- Avaliação por **controle**
- 6 níveis de capacidade

Maturidade

- Relação entre implementação e capacidade
- 5 faixas de maturidade

iSeg & iPriv

Capítulo 6 – Maturidade
Avaliação da Implementação

1. Avaliação da implementação por Medida

Nível de Implementação	Descrição	Pontuação
Adota em maior parte ou totalmente	Há decisão formal ou plano aprovado, e a medida é implementada integralmente em maioria (mais de 50%) ou em todos os ativos de informação da organização.	1
Adota em menor parte	Há decisão formal ou plano aprovado, e a medida na organização é implementada integralmente em menos de 50% dos: - ativos no caso de medida de segurança da informação; ou - processos/serviços no caso de medida de privacidade.	0,75
Adota parcialmente	Há decisão formal ou plano aprovado, e a medida na organização é implementada parcialmente em mais de 50% ou em todos os: - ativos no caso de medida de segurança da informação; ou - processos/serviços no caso de medida de privacidade.	0,5
Há decisão formal ou plano aprovado para adotá-la	Há decisão formal ou plano aprovado, porém não há na organização implementação ou está parcialmente implementado em menos de 50% dos: - ativos no caso de medida de segurança da informação; ou - processos/serviços no caso de medida de privacidade.	0,25
A organização não adota essa medida	Não há qualquer decisão formal ou plano aprovado, tampouco implementação da medida.	0
Não se aplica	A medida não se aplica em nenhum ativo, por entendimento dos gestores ou considerando alguma particularidade do contexto de atuação da organização. **A não aplicabilidade deverá seguir de uma motivação baseada em análise de riscos**.	-

Capítulo 6 – Maturidade
Avaliação da Capacidade

2. Avaliação da capacidade por Controle

Nível de Capacidade	Descrição	Pontuação
0	Ausência de capacidade para a implementação das medidas do controle, ou desconhecimento sobre o atendimento das medidas.	0
1	O controle atinge mais ou menos seu objetivo, por meio da aplicação de um conjunto incompleto de atividades que podem ser caracterizadas como iniciais ou intuitivas (pouco organizadas).	20%
2	O controle atinge seu objetivo por meio da aplicação de um conjunto básico, porém completo, de atividades que podem ser caracterizadas como realizadas.	40%
3	O controle atinge seu objetivo de forma muito mais organizada utilizando os recursos organizacionais. Além disso, **o controle é formalizado por meio de uma política institucional**, específica ou como parte de outra maior.	60%
4	O controle atinge seu objetivo, é bem definido e suas **medidas são implementadas continuamente por meio de um processo** decorrente da política formalizada.	80%
5	O controle atinge seu objetivo, é bem definido, suas medidas são implementadas continuamente por meio de um processo e **seu desempenho é mensurado quantitativamente por meio de indicadores**.	100%

Capítulo 6 – Maturidade
Avaliação da Maturidade

3. Avaliação da maturidade por <u>Controle</u>

Nível de Maturidade	Descrição
0,00 a 0,29	Inicial
0,30 a 0,49	Básico
0,50 a 0,69	Intermediário
0,70 a 0,89	Em Aprimoramento
0,90 a 1,00	Aprimorado

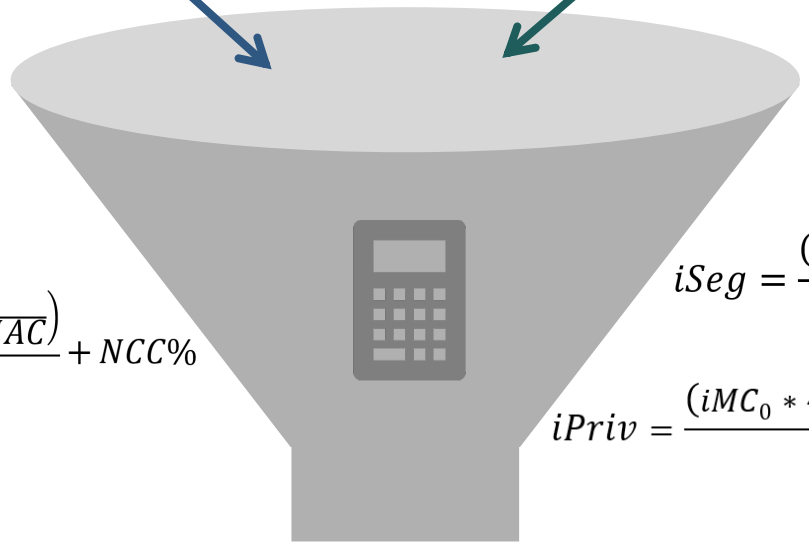
4. Indicador de Maturidade de Segurança (iSeg)

4. Indicador de Maturidade de Privacidade (iPriv)

Capítulo 6 – Maturidade
Resultado

Implementação

Capacidade



$$iMC = \frac{\left(\frac{\sum PMC}{QMC - QMNAC}\right)}{2} + NCC\%$$

$$iSeg = \frac{(iMC_0 * 4) + \sum_{i=1}^{18} iMC_i}{22}$$

$$iPriv = \frac{(iMC_0 * 4) + \sum_{i=19}^{31} iMC_i}{17}$$

Nível de maturidade para cada um dos 31 controles

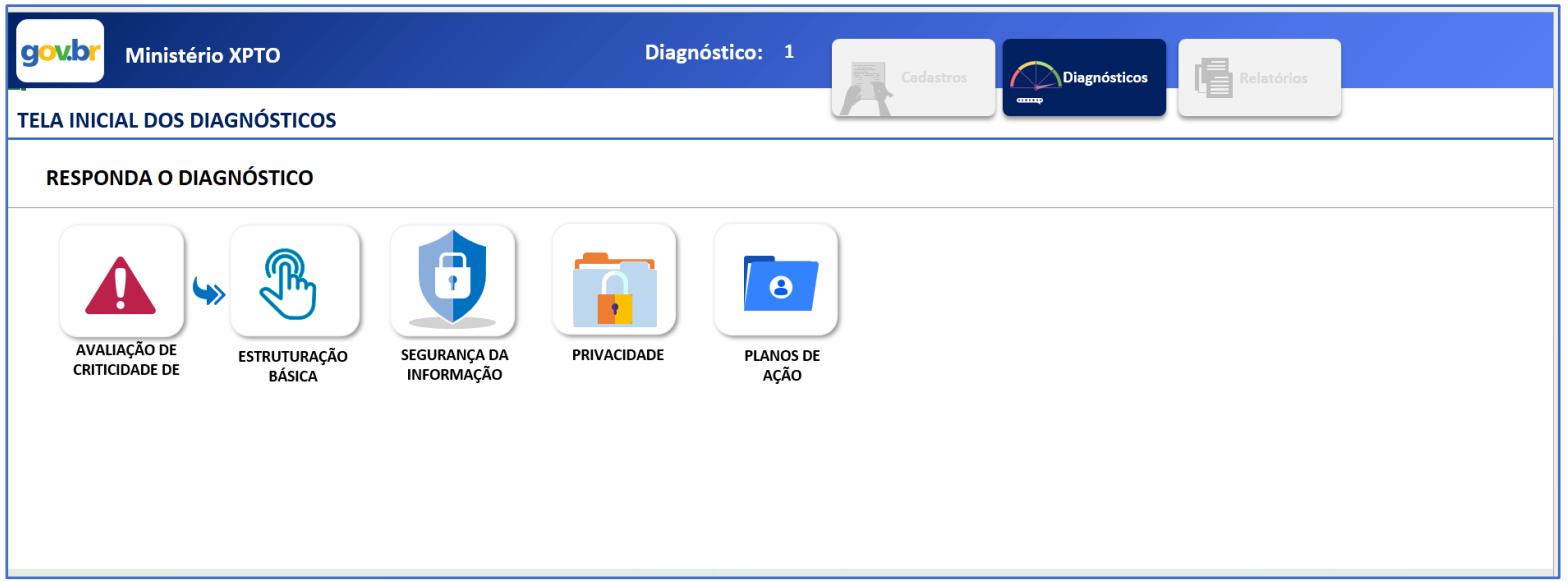
iPriv = Nível de maturidade geral de Privacidade

iSeg = Nível de maturidade geral de Segurança da Informação

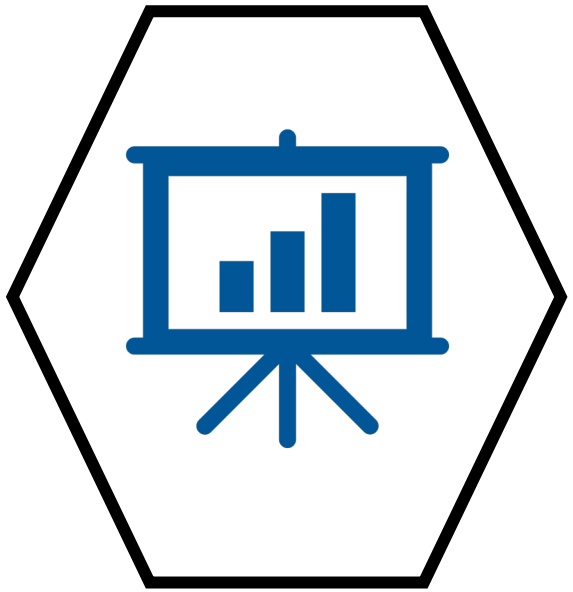
Capítulo 7 - Ferramenta de acompanhamento da implementação do Framework

Ressalta que a SGD desenvolveu uma ferramenta em formato de planilha para automação do Framework, destacando o link para download.

A ferramenta tem um manual próprio a fim de orientar seu uso.



Capítulo 8 – Considerações Finais

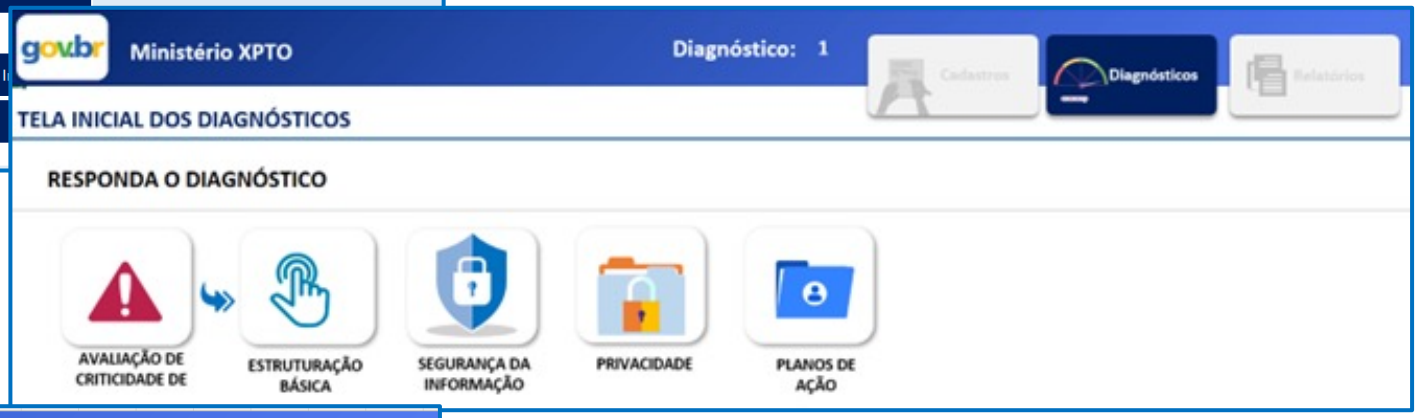


Benefícios

- ✓ **Ampliação da confiabilidade e da proteção de sistemas informáticos** contra os principais ataques que podem resultar em incidentes de segurança.
- ✓ **Aprimoramento da privacidade e da proteção dos dados pessoais dos cidadãos** inseridos nas bases de dados governamentais.
- ✓ **Aumento da confiança da população** nos serviços digitais prestados pelo governo federal.
- ✓ **Disseminação da cultura** de privacidade e segurança da informação nas instituições.
- ✓ **Criação de uma linguagem comum** de controles e de medidas de privacidade e segurança para os órgãos do SISP e demais partes interessadas; e
- ✓ **Aumento da confiança mútua para compartilhamento de dados** entre as **instituições públicas** devido a **evolução dos níveis de maturidade** em privacidade e segurança da informação dos ambientes tecnológicos.

Ferramenta de Automação do Framework

Ferramenta de Automação do Framework
Visão Geral



Obrigado!

Departamento de Privacidade e Segurança da Informação

cgpd@economia.gov.br

(61) 2020-2046