

# **Manual do Usuário da Ferramenta do Framework de Privacidade e Segurança da Informação - Ciclo 1**

## **PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO (PPSI)**

**Versão 3.0**

**Brasília, outubro de 2023**

**MANUAL DO USUÁRIO DA FERRAMENTA DO FRAMEWORK DE PRIVACIDADE E  
SEGURANÇA DA INFORMAÇÃO – CICLO 1**

**MINISTÉRIO DA GESTÃO E INOVAÇÃO EM SERVIÇOS PÚBLICOS**

**Esther Dweck**

Ministra

**SECRETARIA DE GOVERNO DIGITAL**

**Rogério Souza Mascarenhas**

Secretário de Governo Digital

**DEPARTAMENTO DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO**

**Leonardo Rodrigo Ferreira**

Diretor do Departamento de Privacidade e Segurança da Informação

**COORDENAÇÃO-GERAL DE PROTEÇÃO DE DADOS**

**Loriza Andrade Vaz de Melo**

Coordenadora-Geral de Proteção de Dados

**EQUIPE TÉCNICA DE ELABORAÇÃO**

Adriano de Andrade Moura

Amaury C. da Silveira Junior

Bruno Pierre Rodrigues de Sousa

Erion Dias Monteiro

Heráclito Ricardo Ferreira Gomes

Valdecy Oliveira de Araújo

Yuri Arcanjo De Carvalho

**EQUIPE TÉCNICA DE ATUALIZAÇÃO**

Denis Marcelo de Oliveira

Flavia Patrícia Donata Vieira

Gustavo Vieira Isobe de Macedo

Wellington Francisco Pinheiro de Araujo

## Histórico de Versões

Data	Versão	Descrição
01/11/2022	1.0	Primeira versão - Manual do Usuário Ferramenta (PPSI)
01/09/2023	2.0	Segunda versão - Manual do Usuário Ferramenta (PPSI)
01/10/2023	3.0	Terceira versão - Manual do Usuário Ferramenta (PPSI)

# SUMÁRIO

<b>AVISO PRELIMINAR E AGRADECIMENTOS .....</b>	<b>5</b>
<b>1. INTRODUÇÃO.....</b>	<b>6</b>
<b>2. FERRAMENTA E ESTRUTURAÇÃO BÁSICA DE GESTÃO .....</b>	<b>7</b>
<b>3. CADASTRO DO ÓRGÃO .....</b>	<b>8</b>
3.1 ADICIONAR CONTATOS E NOTA TÉCNICA .....	8
3.2 ESTRUTURAÇÃO BÁSICA DE GESTÃO EM PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO .....	9
3.3 DIAGNÓSTICO DE SEGURANÇA DA INFORMAÇÃO.....	10
3.4 DIAGNÓSTICO DE PRIVACIDADE .....	11
3.5 LEGENDA DA LISTA DE OPÇÃO DE RESPOSTA .....	12
3.6 LISTA DE RESPOSTAS DOS DIAGNÓSTICOS DE SI E PRIVACIDADE .....	12
3.7 LISTA DE RESPOSTAS QUALITATIVA.....	13
3.8 PLANOS DE TRABALHO.....	15
3.8.1 <i>Descrição de cada coluna:</i> .....	16
.....	16
<b>4. RELATÓRIOS.....</b>	<b>18</b>
4.1.1 <i>Quais são as opções de implementação?</i> .....	19

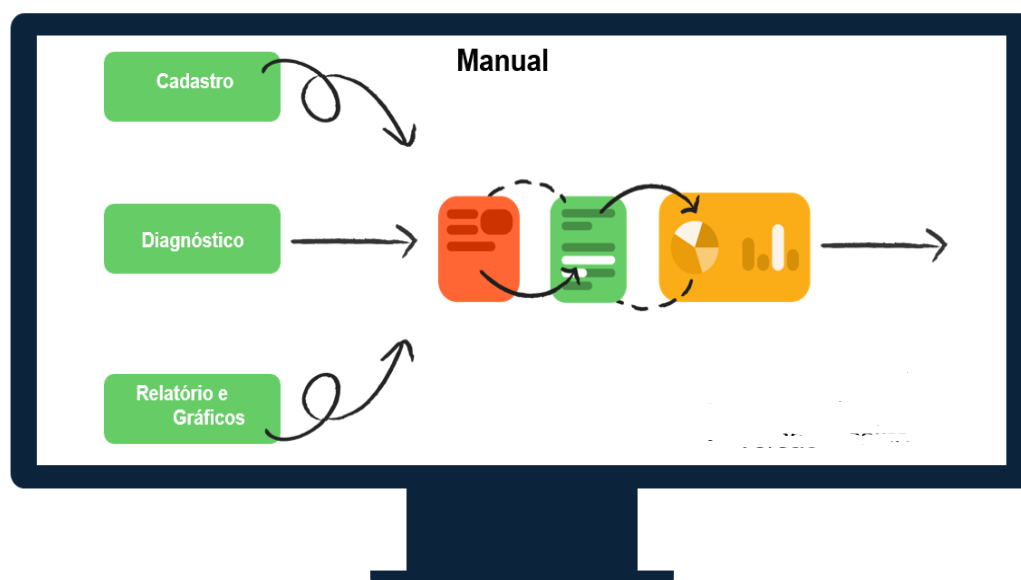
## **AVISO PRELIMINAR E AGRADECIMENTOS**

Este manual visa orientar os usuários na utilização das funcionalidades da Ferramenta do Framework de Privacidade e Segurança da Informação (PPSI) na versão 3.0, que pode ser utilizada amplamente e está otimizada para o ciclo 1 do PPSI. Agradecemos aos órgãos e entidades da Administração Pública Federal (APF) pela aplicação desta ferramenta em prol da privacidade, proteção de dados e segurança da informação.

## 1. INTRODUÇÃO

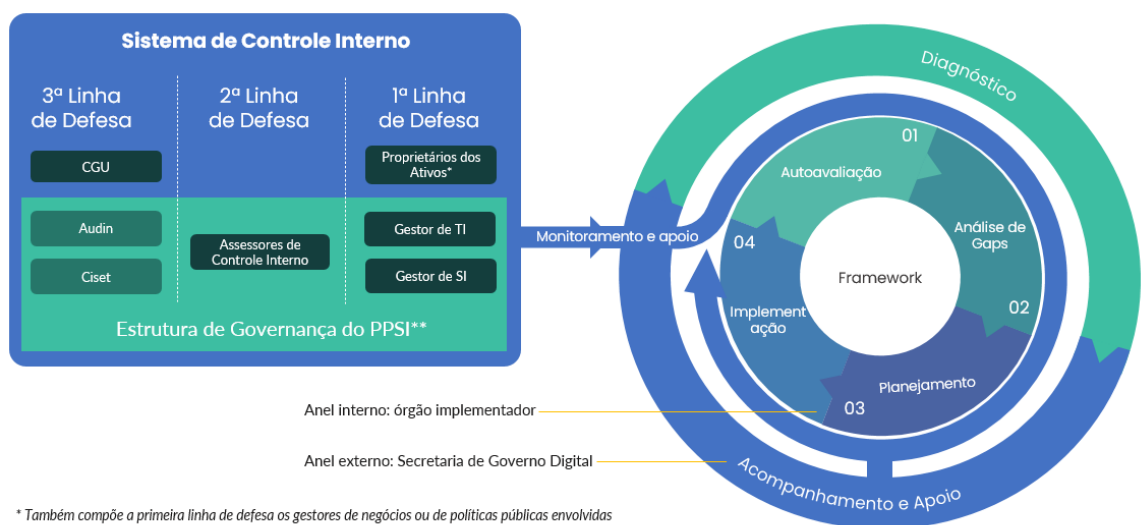
O Manual do Usuário da Ferramenta do Framework de Privacidade e Segurança da Informação é uma fonte de orientação para utilizar a ferramenta descrita no capítulo 7 do Guia do Framework de Privacidade e Segurança da Informação, da Secretaria de Governo Digital (SGD), que faz parte dos guias operacionais elaborados pelo Ministério da Gestão e da Inovação em Serviços Públicos.

Este Manual será periodicamente atualizado para acompanhar o amadurecimento dos processos de privacidade e segurança da informação.



## 2. FERRAMENTA E ESTRUTURAÇÃO BÁSICA DE GESTÃO

A Figura abaixo resume a metodologia de implementação a ser empregada na aplicação do Framework mostrando como estão relacionados o Sistema de Controle Interno (SCI) com os principais atores e as atividades a serem executadas.



\* 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

### 3. CADASTRO DO ÓRGÃO

#### 3.1 Adicionar Contatos

The screenshot displays the 'CADASTROS' (Registers) form within the NBR system. The form is divided into several sections for data entry:

- Top Navigation:** Includes a 'MENU' bar with icons for 'CADASTROS', 'Diagnóstico ESTRUTURA', 'Diagnóstico SEGURANÇA', 'Diagnóstico PRIVACIDAD', 'RELATÓRIO', and 'PLANO DE TRABALHO'.
- Form Fields:**
  - Nome do Responsável pela Unidade de Controle Interno:** Text input field.
  - E-mail do Respondente:** Text input field with placeholder 'Nome\_Responsavel@orgao.com'.
  - Nome do Encarregado pelo Tratamento de Dados Pessoais:** Text input field with placeholder 'Nome\_Responsavel\_Privacidade'.
  - E-mail do Respondente:** Text input field with placeholder 'Nome\_Responsavel@orgao.com'.
  - Nome do Gestor de Segurança da Informação:** Text input field with placeholder 'Nome\_Responsavel\_SI'.
  - E-mail do Respondente:** Text input field with placeholder 'Nome\_Responsavel@orgao.com'.
  - Nome do Gestor de Tecnologia da Informação:** Text input field with placeholder 'Nome\_Responsavel\_TI'.
  - E-mail do Respondente:** Text input field with placeholder 'Nome\_Responsavel@orgao.com'.
  - OUTROS:**
    - Nome do Órgão:** Text input field with placeholder '\*'.
    - CNPJ:** Text input field with placeholder '\*'.
  - USO DA SGD:**
    - Nº do Documento (Nota Técnica):** Text input field.
    - Versão do Diagnóstico enviado:** Text input field.
    - Data Limite para retorno do Diagnóstico:** Text input field.
  - ÁREAS DE DOMÍNIO - PLANO DE TRABALHO:** A table with two columns: 'Responsável' and 'Departamento'. It contains three rows of example data.
 

Responsável	Departamento
EXEMPLO_NOME_RESPONSÁVEL_1	EXEMPLO_NOME_DEPARTAMENTO_1
NOME_RESPONSÁVEL_2	NOME_DEPARTAMENTO_2
NOME_RESPONSÁVEL_3	NOME_DEPARTAMENTO_3
  - DADOS DO RETORNO DO DIAGNÓSTICO PARA SGD:**
    - Data de retorno do Diagnóstico para SGD:** Text input field.
    - Versão do Diagnóstico devolvido:** Text input field.

Para assegurar a exatidão e uniformidade nas informações enviadas à SGD, é fundamental seguir cuidadosamente as orientações ao preencher os campos provenientes da planilha. Insira o nome do responsável pela Unidade de Controle Interno junto com o correspondente endereço de e-mail. De maneira similar, registre o nome do Gestor de Segurança da Informação com seu e-mail associado e assim por diante para os demais campos. No campo "OUTROS", inclua com precisão o nome do órgão na área designada e, quando pertinente, informe o CNPJ. Na seção "ÁREAS DE DOMÍNIO - PLANO DE TRABALHO", forneça minuciosamente os detalhes do responsável. No campo "DADOS DO RETORNO DO DIAGNÓSTICO PARA SGD", forneça detalhes específicos, incluindo a data de retorno do diagnóstico, a versão devolvida e outras informações requisitadas.



### 3.2 Estruturação básica de gestão em privacidade e segurança da informação

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

Selecione de (0 a 5) o Nível de Capacidade do Controle  
RESPOSTA DA VISÃO MACRO DO CONTROLE

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.

ID	MEDIDA	DESCRIÇÃO	RESPOSTA DAS MEDIDAS
0.1	O órgão nomeou uma autoridade máxima de Tecnologia da Informação?	A autoridade máxima de Tecnologia da Informação é responsável secundário por planejar, implementar e melhorar continuamente os controles de privacidade e segurança da informação em soluções de tecnologia da informação e comunicações, nos termos da Instrução Normativa SGD/ME nº 01, de 4 de abril de 2019, e suas alterações, considerando a cadeia de suprimentos relacionada à solução.	Não

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

Selecione de (0 a 5) o Nível de Capacidade do Controle  
RESPOSTA DA VISÃO MACRO DO CONTROLE

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.

ID	MEDIDA	DESCRIÇÃO	RESPOSTA DAS MEDIDAS
0.1	O órgão nomeou uma autoridade máxima de Tecnologia da Informação?	A autoridade máxima de Tecnologia da Informação é responsável secundário por planejar, implementar e melhorar continuamente os controles de privacidade e segurança da informação em soluções de tecnologia da informação e comunicações, nos termos da Instrução Normativa SGD/ME nº 01, de 4 de abril de 2019, e suas alterações, considerando a cadeia de suprimentos relacionada à solução.	Não



É imprescindível o preenchimento do nível de capacidade e de todas suas medidas.

### 3.3 Diagnóstico de Segurança da Informação

ID	ID CIS 8	GRUPO	FUNÇÃO NIST CSF	MEDIDA	RESPOSTA DAS MEDIDAS	RESPOSTA DA VISÃO MACRO DOS CONTROLES
<b>1 CIS CONTROLE 1: INVENTÁRIO E CONTROLE DE ATIVOS INSTITUCIONAIS</b>						
11	11	G1	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 dados. 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 móveis que não estejam sob controle do órgão. Revisar e atualizar o inventário semestralmente ou com mais frequência.	Selecione a Resposta
12	14	G2	IDENTIFICAR	O órgão usa o Dynamic Host Configuration Protocol (DHCP) para Atualizar o Inventário de Ativos?	Utilizar o registro (logs) do Dynamic Host Configuration Protocol (DHCP) em todos os servidores DHCP para utilizar uma ferramenta de gerenciamento de endereços IP para atualizar o inventário de ativos de hardware da instituição.	Selecione a Resposta
13	13	G2	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.	Selecione a Resposta

O diagnóstico de **Segurança da Informação** busca identificar ativos, mitigar riscos e garantir a continuidade das operações.

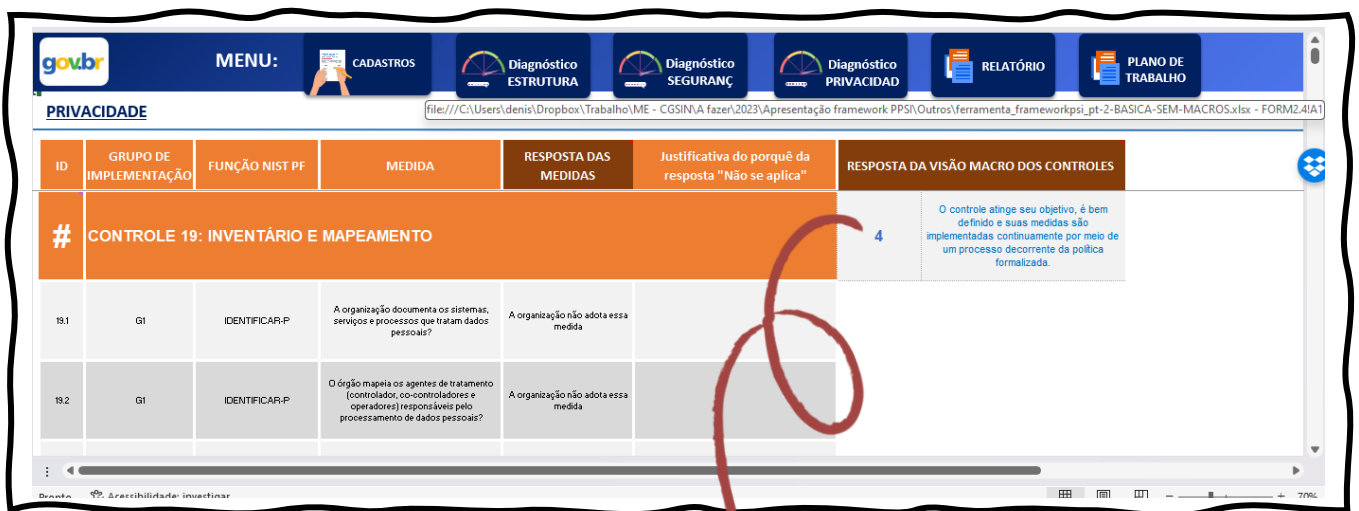
ID	ID CIS 8	GRUPO	FUNÇÃO NIST CSF	MEDIDA	RESPOSTA DAS MEDIDAS	RESPOSTA DA VISÃO MACRO DOS CONTROLES
<b>1 CIS CONTROLE 1: INVENTÁRIO E CONTROLE DE ATIVOS INSTITUCIONAIS</b>						
11	11	G1	IDENTIFICAR	O órgão estabelece e mantém um inventário detalhado de ativos institucionais?	Estabelecer e manter um inventário preciso, detalhado e atualizado de todos os ativos institucionais com potencial para armazenar ou processar dados. 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 móveis que não estejam sob controle do órgão. Revisar e atualizar o inventário semestralmente ou com mais frequência.	Selecione a Resposta
12	14	G2	IDENTIFICAR	O órgão usa o Dynamic Host Configuration Protocol (DHCP) para Atualizar o Inventário de Ativos?	Utilizar o registro (logs) do Dynamic Host Configuration Protocol (DHCP) em todos os servidores DHCP para utilizar uma ferramenta de gerenciamento de endereços IP para atualizar o inventário de ativos de hardware da instituição.	Selecione a Resposta
13	13	G2	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.	Selecione a Resposta



É imprescindível o preenchimento do nível de capacidade e de todas suas medidas.

### 3.4 Diagnóstico de Privacidade

O diagnóstico de **Privacidade** busca mapear, gerir e conscientizar o uso de dados pessoais de forma correta.



ID	GRUPO DE IMPLEMENTAÇÃO	FUNÇÃO NIST PF	MEDIDA	RESPOSTA DAS MEDIDAS	Justificativa do porquê da resposta "Não se aplica"	RESPOSTA DA VISÃO MACRO DOS CONTROLES	
#	CONTROLE 19: INVENTÁRIO E MAPEAMENTO					4	O controle atinge seu objetivo, é bem definido e suas medidas são implementadas continuamente por meio de um processo decorrente da política formalizada.
19.1	G1	IDENTIFICAR-P	A organização documenta os sistemas, serviços e processos que tratam dados pessoais?	A organização não adota essa medida			
19.2	G1	IDENTIFICAR-P	O órgão mapeia os agentes de tratamento (controlador, co-controladores e operadores) responsáveis pelo processamento de dados pessoais?	A organização não adota essa medida			



É imprescindível o preenchimento do nível de capacidade e de todas suas medidas.

### 3.5 Legenda da Lista de Opção de Resposta

**Controles CIS Versão 8**

FILTRO	ID	ID CIS	GRUPO IMPL	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	RESPOSTAS	JUSTIFIQUE, SE A RESPOSTA FOR "NÃO SE APLICA"	Questionário Qualitativo
5						<b>CIS CONTROLE 5: GESTÃO DE CONTAS</b>			2
5	5.1	5.1	G1	IDENTIFICAR	O órgão estabelece e mantém um inventário de contas?	Estabelecer e manter um inventário de todas as contas gerenciadas na organização. O inventário deve incluir contas de usuário e administrador. Validar se todas as contas ativas estão autorizadas, trimestralmente ou com mais frequência.	Selecione a Resposta		O controle atinge seu objetivo por meio da aplicação de um conjunto básico, porém completo, de atividades que podem ser caracterizadas como realizadas.
					O órgão estabelece e mantém	Estabelecer e manter um inventário de contas de serviço. O inventário, no mínimo, deve conter o departamento proprietário, data de revisão e	Adota em maior parte ou totalmente Adota parcialmente Há decisão formal ou plano aprovado A organização não adota essa Não se aplica		

### 3.6 Lista de Respostas dos Diagnósticos de SI e Privacidade

**RESPOSTAS**

JUSTIFIQUE, SE A RESPOSTA FOR "NÃO SE APLICA"

Selecione a Resposta

Selecione a Resposta

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

A **lista de respostas** será a mesma para os Diagnósticos de Segurança da Informação e Privacidade.



#### Nível de Implementação

#### Descrição

##### Adota em maior parte ou totalmente

Há decisão formal ou plano aprovado, e a medida na organização é implementada integralmente 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.

##### 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.

##### 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.

<b>Há decisão formal ou plano aprovado para implementar</b>	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.
<b>A organização não adota essa medida</b>	Não há qualquer decisão formal ou plano aprovado, tampouco implementação da medida.
<b>Não se aplica</b>	A medida não se aplica em nenhum ativo no caso de medida de segurança da informação ou processo/serviço no caso de medida de privacidade, por entendimento dos gestores ou considerando alguma particularidade do contexto de atuação da organização. A não aplicabilidade deverá seguir de uma motivação baseada em uma análise de riscos.

### 3.7 Lista de Respostas Qualitativa



**Questionário Qualitativo**

1

Selecione sua Resposta

0

1

2

3

4

5

iniciais ou intuitivas (pouco organizadas).

O questionário qualitativo consta no **Diagnósticos de Segurança da Informação e Privacidade.**



O nível de capacidade foca no aspecto qualitativo, e tem como objetivo avaliar o nível de efetividade da adequação de um controle. O avaliador deverá considerar um dos níveis de capacidade a seguir para cada controle.

Nível de Capacidade	Descrição
0	Ausência de capacidade para a implementação das medidas do controle, ou desconhecimento sobre o atendimento das medidas.
1	O controle atinge mais ou menos seu objetivo, por meio da implementação de um conjunto incompleto de atividades que podem ser caracterizadas como iniciais ou intuitivas (pouco organizadas).
2	O controle atinge seu objetivo por meio da implementação de um conjunto básico, porém completo, de atividades que podem ser caracterizadas como realizadas.
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.
4	O controle atinge seu objetivo, é bem definido e suas medidas são implementadas continuamente por meio de um processo decorrente da política formalizada.
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.

**FIQUE ATENTO!**

As respostas influenciam no cálculo da maturidade, ou seja, é importante avaliar em qual das opções de descrição melhor responde a medida do formulário.



Após preenchimento dos formulários, é importante observar que as medidas não implementadas irão compor o plano de Trabalho. Possibilitando, assim, a implementação de ações que melhorem a maturidade do respectivo controle.

### 3.8 Planos de Trabalho



ID	MEDIDA	RESPOSTA	Encaminhamento Interno (para uso do órgão)	Responsáveis	Departamento	Observação do Órgão para SGD	Previsão de Início	Previsão de Término
0.1	O órgão nomeou uma autoridade máxima de Tecnologia da Informação?	Selecione a Opção			Selecione Responsável			
0.2	O órgão nomeou um Gestor de Segurança da Informação?	Selecione a Opção			Selecione Responsável			
0.3	O órgão nomeou um responsável pela unidade de controle interno?	Selecione a Opção			Selecione Responsável			
0.4	O órgão instituiu um Comitê de Segurança da Informação?	Selecione a Opção			Selecione Responsável			
0.5	O órgão instituiu uma Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETRC?	Selecione a Opção			Selecione Responsável			

O **plano de trabalho** é uma lista, onde é possível criar e gerenciar prazos, prioridades, informar responsáveis e alterar respostas.

### AVISO!!!

Ao ter acesso ao formulário pela **primeira vez para avaliar** os planos de Trabalho é importante clicar no botão "**Planos de Trabalho**", e então preencher os demais campos do formulário do plano de Trabalho.

### 3.8.1 Descrição de cada coluna:



1	2	3	4	5	6	7	8	9	10	11	12	13
ID	MEDIDA	RESPOSTA	Encaminhamento interno (o órgão faz o preenchimento manual)	Responsável	Departamento	Observação do Órgão p SGO	Previsão de Início	Previsão de Fim	Status DA Medida	Status Medida	Nova resposta	Prioridade
0.3	O órgão nomeou um responsável pela unidade de controle interno?	Não	FRAMEWORK	SALA-01	SGD-OS	04/09/2022	10/09/2022	Atrasado	Não Finalizado	Sim	Não	Não
0.4	O órgão instituiu um Comitê de Segurança da Informação?	Não	FRAMEWORK	SURICATO-02	SALA-02	SGD-OBSERVAÇÃO	05/09/2022	10/09/2022	Atrasado	Não	Não	Não
0.5	O órgão instituiu uma Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR?	Não	FRAMEWORK	SURICATO-03	SALA-03	SGD-OBSERVAÇÃO	06/09/2022	10/09/2022	Concluído	Finalizado	Não	Sim
0.6	O órgão elaborou uma Política de Segurança da Informação - POSIN?	Não	FRAMEWORK	SURICATO-04	SALA-04	SGD-OBSERVAÇÃO	07/09/2022	10/09/2022	Concluído	Finalizado	Não	Sim
...	O órgão nomeou um Encarregado pelo											

ITEM	NOME	DESCRIÇÃO	RECOMENDAÇÃO
1	ID	É o código identificador da medida	Não precisa de atuação do usuário final.
2	MEDIDA	Descrição da Medida	Não precisa de atuação do usuário final.
3	RESPOSTA	É a resposta que foi preenchida no diagnóstico	Não precisa de atuação do usuário final.
4	ENCAMINHAMENTO INTERNO	O órgão preencherá esse campo com as informações de direcionamento dos planos de ação, para que a maturidade possa ser melhorada.	É opcional o preenchimento desse campo.
5	RESPONSÁVEL	O órgão selecionará na lista de responsáveis, no qual foi preenchida no cadastro, com o objetivo de direcionar para o responsável pelo o plano de trabalho, para que a maturidade possa ser melhorada.	É opcional o preenchimento desse campo.



6	<b>DEPARTAMENTO</b>	O departamento é um campo que foi preenchido no cadastro. Está associado ao responsável do plano de trabalho.	Esse campo é preenchido automaticamente, caso o usuário final tenha selecionado o responsável pelo plano de trabalho.
7	<b>OBSERVAÇÃO DO ÓRGÃO PARA SGD</b>	Serve para que o órgão possa inserir informação a respeito	É opcional o preenchimento desse campo.
8	<b>PREVISÃO DE INÍCIO</b>	Serve para direcionar para o responsável a data inicial do plano de trabalho.	É <b>imprescindível</b> que preencha a data de previsão de início do plano de trabalho
9	<b>PREVISÃO DE FIM</b>	Serve para direcionar para o responsável a data fim do plano de trabalho.	É <b>imprescindível</b> que preencha a data de previsão de fim do plano de trabalho para o funcionamento correto do preenchimento dos dados na ferramenta.
10	<b>STATUS PA</b>	De acordo com a data inicial e a data fim é possível acompanhar o status do plano de trabalho (em andamento, concluído ou atrasado)	Esse campo é preenchido automaticamente após o preenchimento da data de início e fim.
11	<b>STATUS MEDIDA</b>	É um campo que permite controlar o a medida que foi finalizada e a que ainda não foi finalizada.	É <b>imprescindível</b> que selecione uma das duas opções ( <b>finalizado</b> ou <b>não finalizado</b> ) para controle do status do plano de trabalho e outros recursos da ferramenta.
12	<b>NOVA RESPOSTA</b>	Esse campo possibilita após implementar os planos de ações na medida para melhorar a maturidade, mudar a resposta para a nova opção para refletir na resposta do formulário da respectiva medida.	Esse campo é para ser preenchido se o plano de trabalho da medida tiver uma evolução significativa.
13	<b>PRIORIDADE</b>	A lista com as opções de respostas “Sim” ou “Não”, possibilita ao respondente indicar se a medida é prioridade. <b>Todas as medidas do controle 0 serão prioridades.</b> Será emitido uma nota técnica no qual vai indicar os controles de segurança da informação e privacidade que serão prioridades também.	A resposta para esse campo será preenchida pelo respondente responsável por direcionar os planos de ação.

## 4. RELATÓRIOS

**RELATÓRIO DE TODOS OS CONTROLES**

ID CONTROLE	NOME CONTROLE	Indicador de Maturidade do Controle de Estruturação Básica	Nível de Maturidade
0	ESTRUTURAÇÃO BÁSICA DE GESTÃO EM SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE	0,14	Inicial
<b>ISEG</b>		<b>0,04</b>	<b>Inicial</b>

ID CONTROLE	NOME CONTROLE	Indicador de Maturidade do Controle de Segurança da Informação	Nível de Maturidade
1	CIS CONTROLE 1: INVENTÁRIO E CONTROLE DE ATIVOS INSTITUCIONAIS	0,32	Básico
2	CIS CONTROLE 2: INVENTÁRIO E CONTROLE DE ATIVOS DE SOFTWARE	Por favor preencha todas as medidas	Preencha todas as medidas
3	CIS CONTROLE 3: PROTEÇÃO DE DADOS	Por favor preencha todas as medidas	Preencha todas as medidas
4	CIS CONTROLE 4: CONFIGURAÇÃO SEGURA DE ATIVOS INSTITUCIONAIS E SOFTWARE	Por favor preencha todas as medidas	Preencha todas as medidas

### AVISO!!!

*O relatório de todos os controles engloba tanto segurança da informação quanto privacidade e tem como objetivo apresentar de forma consolidada a maturidade de cada controle.*

#### 4.1.1 *Quais são as opções de implementação?*

**Não Adota:** O órgão não adota a medida, ou seja, não há qualquer decisão formal ou plano aprovado, tampouco implementação da medida.

**Não Implementada:** O órgão não implementou a medida, ou seja, a medida foi respondida com algumas das opções abaixo:

**Adota a medida integralmente em menos de 50% dos ativos**

**Adota a medida parcialmente em mais de 50% dos ativos**

**Há decisão formal ou plano aprovado para implementar**

**Implementada:** O órgão implementou a medida, ou seja, a medida foi respondida com “Adota a medida integralmente em mais de 50% dos ativos”. Há decisão formal ou plano aprovado, e a medida é implementada integralmente na maioria (mais de 50%) ou em todos os ativos de informação da organização.

**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 uma análise de riscos.

Com o compromisso contínuo de aprimorar a privacidade e a segurança da informação em nosso ambiente digital, este manual servirá como um guia valioso para os usuários da Ferramenta do Framework de Privacidade e Segurança da Informação. Agradecemos a todos os órgãos e entidades da Administração Pública Federal que buscam promover uma cultura de respeito aos dados pessoais e à proteção da informação.

Estamos empenhados em evoluir junto com os avanços tecnológicos e as mudanças regulatórias, garantindo que esta ferramenta continue a ser uma aliada confiável na busca pela excelência em privacidade e segurança. Desejamos sucesso em suas jornadas e esforços para construir um ambiente digital cada vez mais seguro e respeitoso.

**Dúvida?  
Entre em  
contato  
conosco.**

Email: [cgpd@economia.gov.br](mailto:cgpd@economia.gov.br)

Telefone: (61) 2020-2046



DEPARTAMENTO DE  
**PRIVACIDADE E  
SEGURANÇA DA INFORMTRABALHO**

SECRETARIA DE  
**GOVERNO DIGITAL**

MINISTÉRIO DA  
**GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS**