

**Manual do Usuário da Ferramenta do  
Framework de Privacidade e Segurança  
da Informação -  
Ciclo 3**

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

**Versão 5.0**

**Brasília, junho de 2024**

**MANUAL DO USUÁRIO DA FERRAMENTA DO FRAMEWORK DE PRIVACIDADE E  
SEGURANÇA DA INFORMAÇÃO – CICLO 2**

**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

Ricardo Villas-Bôas Fernandes

Wellington Francisco Pinheiro de Araujo

## Histórico de Versões

<b>Data</b>	<b>Versão</b>	<b>Descrição</b>
<b>01/11/2022</b>	1.0	Primeira versão - Manual do Usuário Ferramenta (PPSI)
<b>01/09/2023</b>	2.0	Segunda versão - Manual do Usuário Ferramenta (PPSI)
<b>01/10/2023</b>	3.0	Terceira versão - Manual do Usuário Ferramenta (PPSI)
<b>10/01/2023</b>	4.0	Quarta versão - Manual do Usuário Ferramenta (PPSI)
<b>28/06/2024</b>	5.0	Quinta versão - Manual do Usuário Ferramenta (PPSI)

# SUMÁRIO

AVISO INICIAL E EXPRESSÃO DE GRATIDÃO.....	5
1. INTRODUÇÃO.....	6
2. FERRAMENTA E ESTRUTURAÇÃO BÁSICA DE GESTÃO .....	7
3. CADASTRO DO ÓRGÃO .....	8
3.1 ADICIONAR CONTATOS .....	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
4. RELATÓRIOS.....	18
MENSAGEM FINAL .....	19

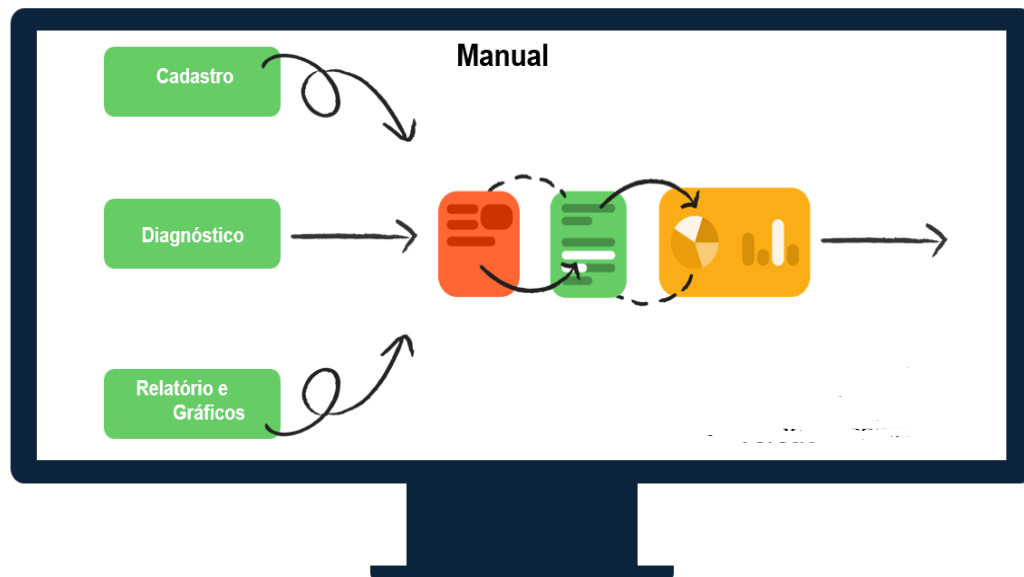
## AVISO INICIAL E EXPRESSÃO DE GRATIDÃO

Este guia tem como propósito oferecer diretrizes abrangentes aos usuários na exploração das funcionalidades da Ferramenta do Framework de Privacidade e Segurança da Informação (PPSI). Esta versão, amplamente aplicável, foi otimizada para atender especificamente ao Ciclo 3 do PPSI. Expressamos nossa sincera gratidão aos órgãos e entidades da Administração Pública Federal (APF) pela dedicação em aplicar esta ferramenta, fortalecendo assim os pilares da privacidade, proteção de dados e segurança da informação.

## 1. INTRODUÇÃO

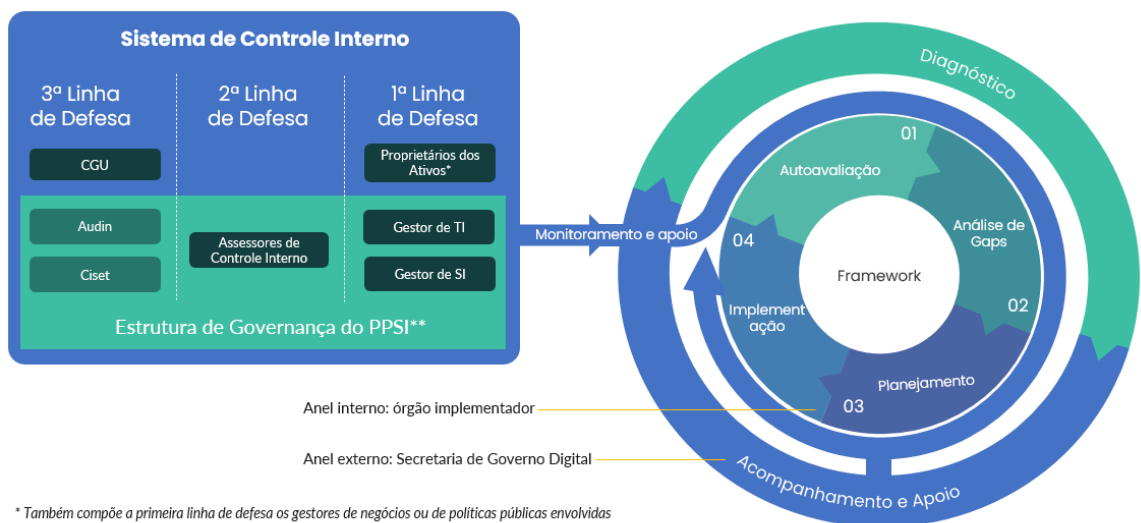
O Manual do Usuário da Ferramenta do Framework de Privacidade e Segurança da Informação é uma fonte abrangente de orientações destinada a facilitar a utilização eficaz da ferramenta mencionada no Capítulo 7 do Guia do Framework de Privacidade e Segurança da Informação da Secretaria de Governo Digital (SGD). Esta ferramenta integra os guias operacionais desenvolvidos pelo Ministério da Gestão e Inovação em Serviços Públicos.

É relevante destacar que este manual será alvo de atualizações periódicas, alinhando-se ao contínuo amadurecimento dos processos relacionados à privacidade e segurança da informação. Estas atualizações visam assegurar que o material permaneça contemporâneo e útil à medida que novas práticas e diretrizes se desenvolvem no cenário da administração pública.



## 2. FERRAMENTA E ESTRUTURAÇÃO BÁSICA DE GESTÃO

A representação visual abaixo encapsula a metodologia de implementação a ser adotada na aplicação do Framework, delineando a interconexão entre o Sistema de Controle Interno (SCI), os principais intervenientes 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 shows a web browser window displaying a 'CADASTROS' (Registers) page. The page has a blue header with a 'MENU' and several icons for 'Diagnóstico ESTRUTURA', 'Diagnóstico SEGURANÇA', 'Diagnóstico PRIVACIDAD', 'RELATÓRIO', and 'PLANO DE TRABALHO'. The main content area is titled 'CADASTROS' and contains several form sections:

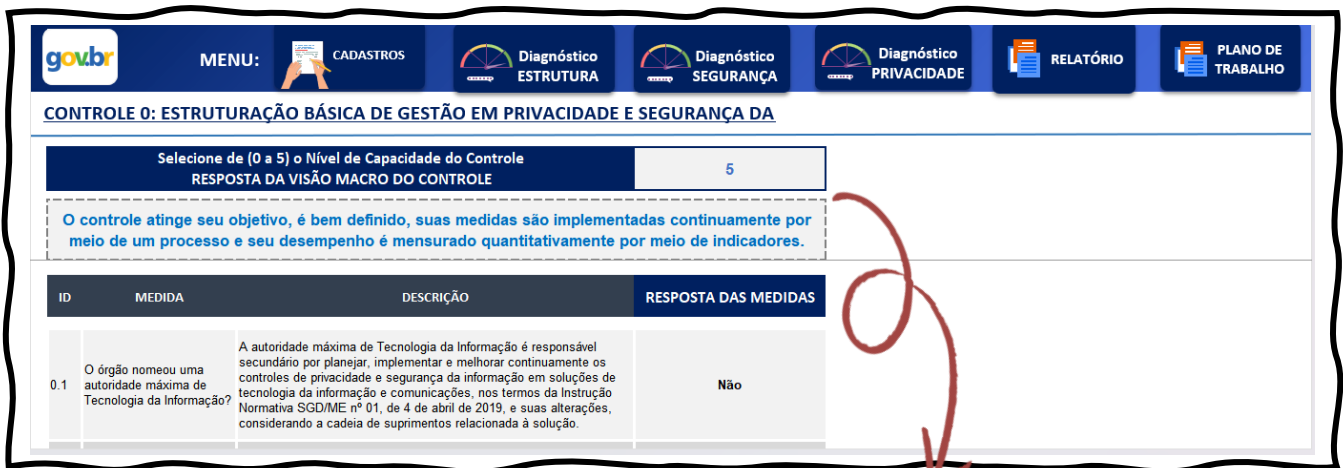
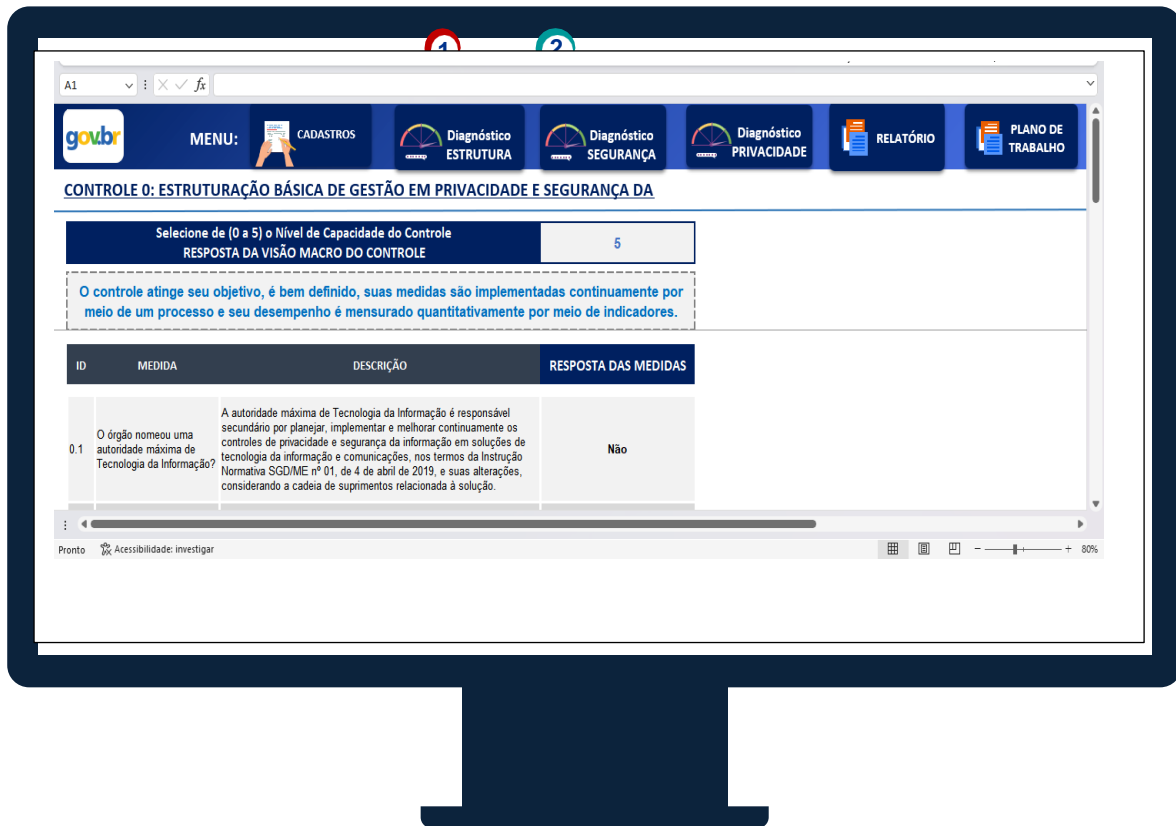
- Nome do Responsável pela Unidade de Controle Interno:** [Input field]
- E-mail do Respondente:** [Input field with placeholder: Nome\_Responsavel@orgao.com]
- Nome do Gestor de Segurança da Informação:** Nome\_Responsavel\_SI
- E-mail do Respondente:** [Input field with placeholder: Nome\_Responsavel@orgao.com]
- Nome do Encarregado pelo Tratamento de Dados Pessoais:** Nome\_Responsavel\_Privacidade
- E-mail do Respondente:** [Input field with placeholder: Nome\_Responsavel@orgao.com]
- Nome do Gestor de Tecnologia da Informação:** Nome\_Responsavel\_TI
- E-mail do Respondente:** [Input field with placeholder: Nome\_Responsavel@orgao.com]
- OUTROS:**
  - Nome do Órgão:** \*
  - CNPJ:** \*
- USO DA SGD:**
  - Nº do Documento (Nota Técnica):** [Input field]
  - Versão do Diagnóstico enviado:** [Input field]
  - Data Limite para retorno do Diagnóstico:** [Input field]
- ÁREAS DE DOMÍNIO - PLANO DE TRABALHO:**

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:** [Input field]
  - Versão do Diagnóstico devolvido:** [Input field]

Para garantir precisão e consistência nas informações enviadas à SGD, é crucial seguir atentamente as orientações ao preencher os campos provenientes da planilha. Inclua o nome do responsável pela Unidade de Controle Interno juntamente com o respectivo endereço de e-mail. Da mesma forma, registre o nome do Gestor de Segurança da Informação com o e-mail associado e repita esse processo para os demais campos. No campo "OUTROS", insira com precisão o nome do órgão na área designada e, quando aplicável, informe o CNPJ. Na seção "ÁREAS DE DOMÍNIO - PLANO DE TRABALHO", forneça detalhes sobre o responsável. No campo "DADOS DO RETORNO DO DIAGNÓSTICO PARA SGD", inclua informações específicas, como a data de retorno do diagnóstico, a versão devolvida e outras informações solicitadas. Isso garantirá a qualidade e integridade das informações enviadas à SGD.

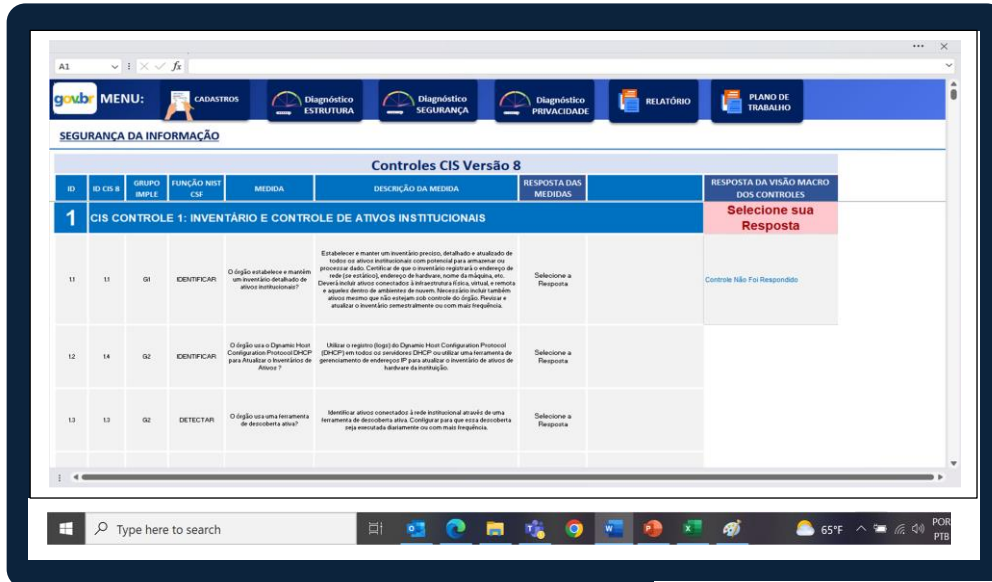


## 3.2 Estruturação básica de gestão em privacidade e segurança da informação

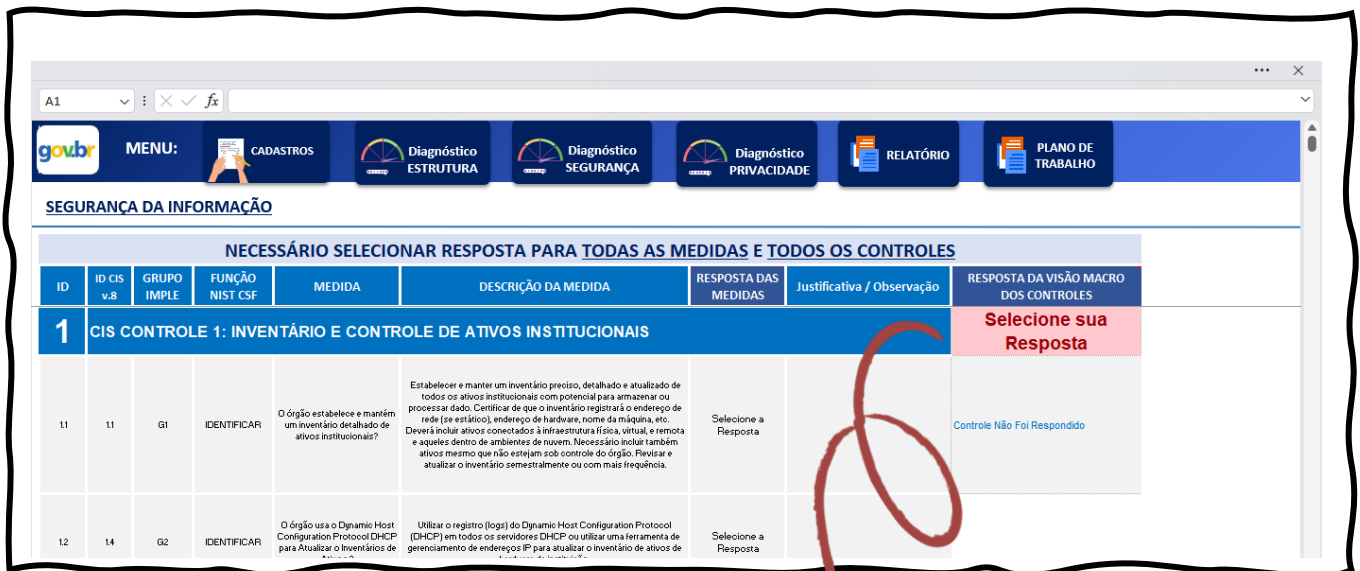


É imprescindível o preenchimento da visão macro do controle e de todas suas medidas.

### 3.3 Diagnóstico de Segurança da Informação



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



É imprescindível o preenchimento da visão macro dos controles 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 / Observação	RESPOSTA DA VISÃO MACRO DOS CONTROLES
<b>19 CONTROLE 19: INVENTÁRIO E MAPEAMENTO</b>						
19.1	G1	IDENTIFICAR-P	A organização documenta os sistemas, serviços e processos que tratam dados pessoais?	Selecione a Resposta		Selecione sua Resposta Controle Não Foi Respondido



É imprescindível o preenchimento da visão macro dos controles e de todas suas medidas.

### 3.5 Legenda da Lista de Opção de Resposta

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

Nível de Implementação	Descrição
<b>Adota em maior parte ou totalmente</b>	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.
<b>Adota em menor parte</b>	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.
<b>Adota parcialmente</b>	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 do Controle	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.

Responda todas as medidas e todos os controles, mesmo que ainda não tenha nada implementado, para o adequado cálculo dos indicadores.



**Planos de Trabalho**

Após preenchimento dos Diagnósticos, é importante observar que as medidas não implementadas totalmente devem compor o Plano de Trabalho. Possibilitando, assim, a implementação de ações que melhorem a maturidade do respectivo controle.

### 3.8 Planos de Trabalho



QTD TOTAL DE MEDIDAS:		310		QTD DE MEDIDAS COM PRIORIDADE:		96					
CICLO	ID	MEDIDA	RESPOSTA	Encaminhamento Interno (para uso do órgão)	Responsáveis	Departamento	Observação do órgão para SGD	Previsão de Início	Pr		
1	0.1	O órgão nomeou uma autoridade máxima de Tecnologia da Informação?	Selecione a Opção			Selecione Responsável					
1	0.2	O órgão nomeou um Gestor de Segurança da Informação?	Selecione a Opção			Selecione Responsável					
1	0.3	O órgão nomeou um responsável pela unidade de controle interno?	Selecione a Opção			Selecione Responsável					
1	0.4	O órgão instituiu um Comitê de Segurança da Informação?	Selecione a Opção			Selecione Responsável					
1	0.5	O órgão instituiu uma Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETR?	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 **“Plano de Trabalho** é fundamental conferir as medidas prioritizadas para o Ciclo atual e os anteriores e então preencher os demais campos do formulário do Plano de Trabalho.

As medidas já prioritizadas para o Ciclo atual ou anteriores que ainda não foram totalmente atendidas devem ser preenchidas com as datas estimadas para a implementação.

### 3.8.1 Descrição de cada coluna:

CICLO		CICLO DE MEDIDAS COM PRIORIDADE		ENCAMINHAMENTO INTERNO (para uso próprio)		Responsável	Departamento	Observação do Órgão para SG	Previsão de Início	Previsão de Fim	Status Plano Anual	Status Medida	Nova resposta	Prioridade
1	0.1	O órgão nomeou uma autoridade máxima de Tecnologia da Informação?	Selecione a Opção				Selecionar Responsável				Atrasado	.		Sim
1	0.2	O órgão nomeou um Gestor de Segurança da Informação?	Selecione a Opção				Selecionar Responsável				Atrasado	.		Sim
1	0.3	O órgão nomeou um responsável pela unidade de controle interno?	Selecione a Opção				Selecionar Responsável				Atrasado	.		Sim
1	0.4	O órgão instituiu um Comitê de Segurança da Informação?	Selecione a Opção				Selecionar Responsável				Atrasado	.		Sim
1	0.5	O órgão instituiu uma Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR?	Selecione a Opção				Selecionar Responsável				Atrasado	.		Sim
1	0.6	O órgão elaborou uma Política de Segurança da Informação - PSDI/PI?	Selecione a Opção				Selecionar Responsável				Atrasado	.		Sim
1	0.7	O órgão nomeou um Encarregado pelo Tratamento de Dados Pessoais?	Selecione a Opção				Selecionar Responsável				Atrasado	.		Sim
1	1.1	O órgão estabelece e mantém um inventário detalhado de ativos institucionais?	Selecione a Resposta				Selecionar Responsável				Atrasado	.		Sim
A Definir	1.2	O órgão usa o Dynamic Host Configuration Protocol DHCP para Atualizar o Inventário de Ativos?	Selecione a Resposta				Selecionar Responsável				Atrasado	.		Não
A Definir	1.3	O órgão usa uma ferramenta de descoberta ativa?	Selecione a Resposta				Selecionar Responsável				Atrasado	.		Não

COLUNA	DESCRIÇÃO	RECOMENDAÇÃO	
1	<b>Ciclo</b>	São os ciclos do plano	Pode ser utilizado para filtrar o ciclo atual.
2	<b>ID</b>	É o código identificador da medida	Não precisa de atuação do usuário final.
3	<b>MEDIDA</b>	Descrição da Medida	Não precisa de atuação do usuário final.
4	<b>RESPOSTA</b>	É a resposta que foi preenchida no diagnóstico (a resposta vem automaticamente quando preenchida no respectivo diagnóstico)	Não precisa de atuação do usuário final.
5	<b>ENCAMINHAMENTO INTERNO</b>	O órgão preencherá esse campo com as informações de direcionamento internos dos planos de ação, para que a maturidade possa ser melhorada.	É opcional o preenchimento desse campo.
6	<b>RESPONSÁVEL</b>	O órgão selecionará na lista de responsáveis, no qual foi preenchida no "Cadastro", com o objetivo de direcionar para o responsável pelo plano de trabalho, para que a maturidade possa ser melhorada.	É opcional o preenchimento desse campo.



	COLUNA	DESCRIÇÃO	RECOMENDAÇÃO
7	<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.
8	<b>OBSERVAÇÃO DO ÓRGÃO PARA SGD</b>	Serve para que o órgão possa inserir informações relevantes à SGD, como justificativas pela não implementação de uma medida já priorizada.	É opcional o preenchimento desse campo na maioria dos casos, devendo ser preenchido quando o prazo de uma medida vencer e ela não for totalmente atendida.
9	<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 para as medidas priorizadas.
10	<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 as medidas priorizadas.
11	<b>STATUS PLANO DE AÇÃO</b>	De acordo com a previsão de início e a previsão de fim é possível acompanhar o status do plano de trabalho (em andamento, concluído ou atrasado)	Esse campo é preenchido automaticamente após o preenchimento da previsão de início e da previsão de fim.
12	<b>STATUS MEDIDA</b>	É um campo que permite controlar 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.
13	<b>NOVA RESPOSTA</b>	Campo legado que foi mantido por questões de compatibilidade entre versões das ferramentas. Futuramente pode vir a ser usado para outras finalidades.	As atualizações de respostas das medidas e controles devem ser realizadas diretamente nos respectivos Diagnósticos.
14	<b>PRIORIDADE</b>	Indica se a medida está priorizada para o Ciclo atual ou anteriores.	A SGD tem fornecido a cada Ciclo do PPSI a ferramenta otimizada já com as medidas priorizadas selecionadas com "Sim" neste campo.

## 4. RELATÓRIOS

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 a estrutura básica, quanto a segurança da informação e a privacidade e tem como objetivo apresentar de forma consolidada a maturidade de cada controle.*

*O relatório avisa textualmente quando algum controle não está com todas as medidas e os controles respondidos.*

*Ao preencher completamente todos os Diagnósticos, o relatório apresentará os valores dos indicadores individuais de cada controle e os valores globais da Estrutura Básica, do iSeg e do iPriv.*

## MENSAGEM FINAL

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.

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

Email: [ppsi.sgd@gestao.gov.br](mailto:ppsi.sgd@gestao.gov.br)

Telefone: (61) 2020-2046



DEPARTAMENTO DE  
PRIVACIDADE E  
SEGURANÇA DA INFORMAÇÃO

SECRETARIA DE  
GOVERNO DIGITAL

MINISTÉRIO DA  
GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS