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

Rogerio 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

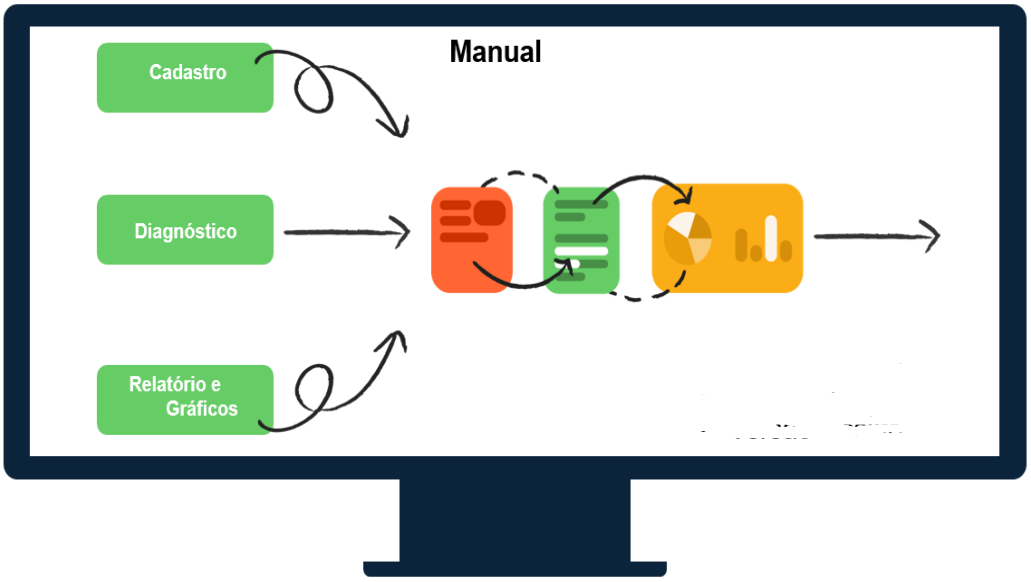
AVISO PRELIMINAR E AGRADECIMENTOS

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

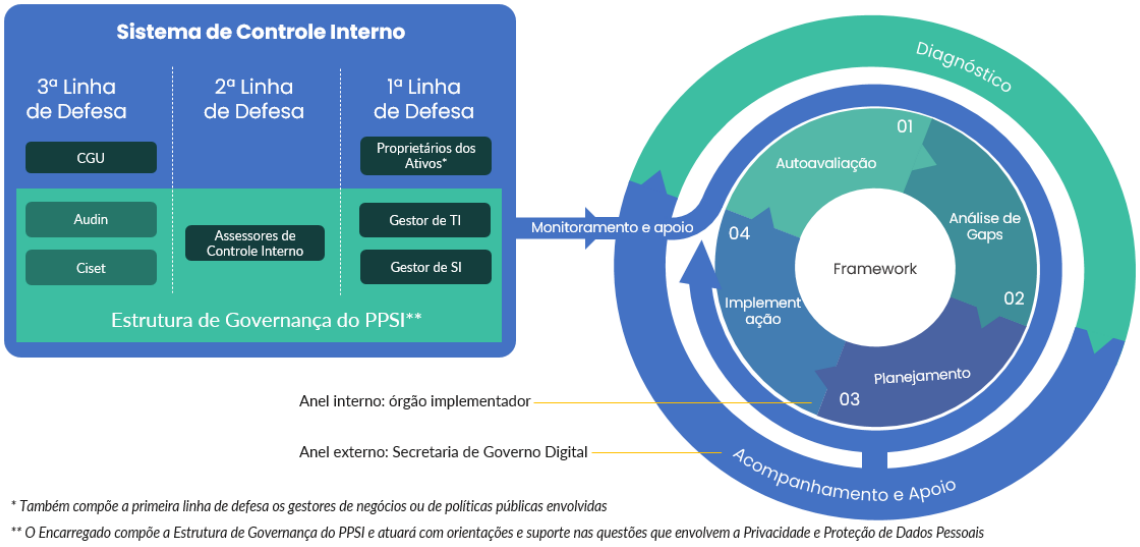
O Manual do Usuário da Ferramenta do Framework de Privacidade e Segurança da Informação é uma fonte de orientação para utilizar a ferramenta descrita no capítulo 7 do Guia do Framework de Privacidade e Segurança da Informação, da Secretaria de Governo Digital (SGD), que faz parte dos guias operacionais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

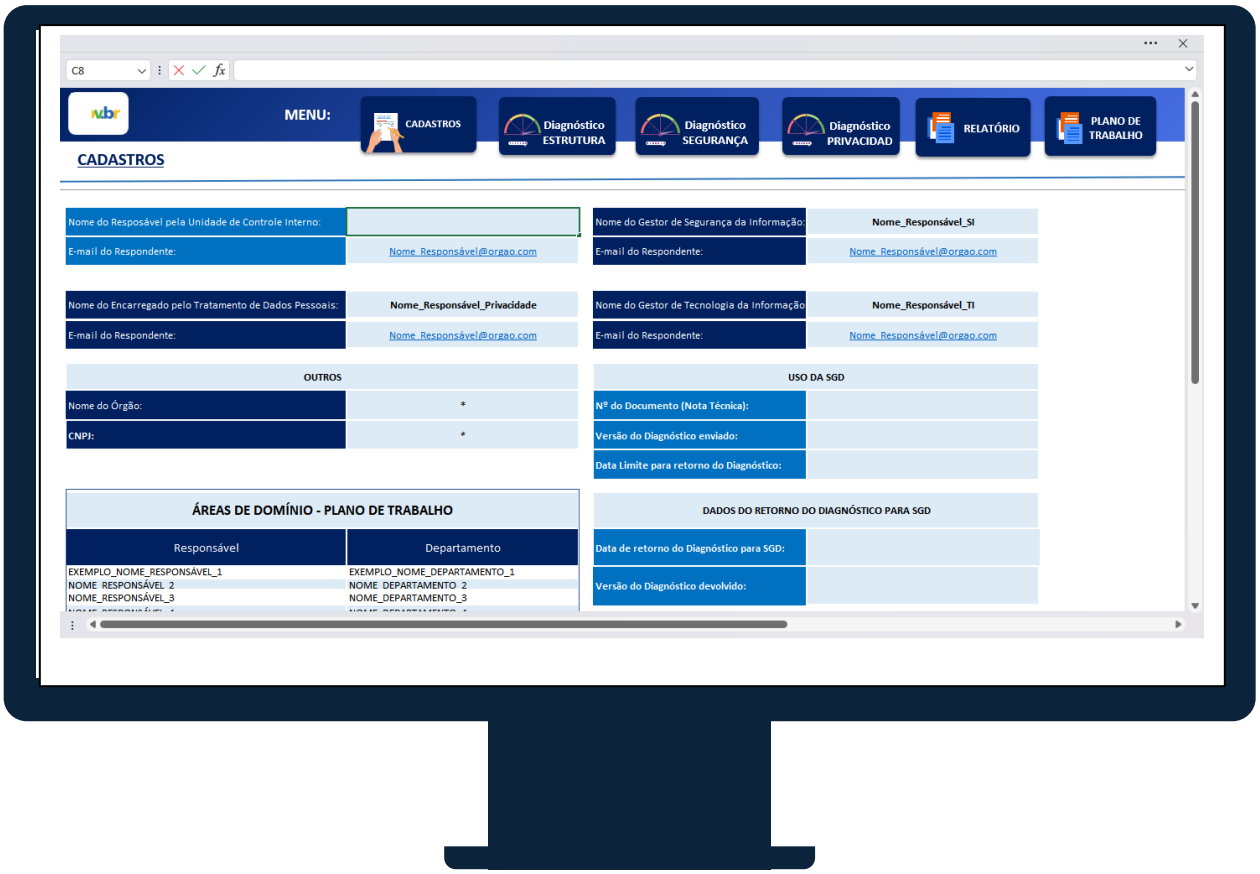


** Também compõe a primeira linha de defesa os gestores de negócios ou de políticas públicas envolvidas*

*** 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*

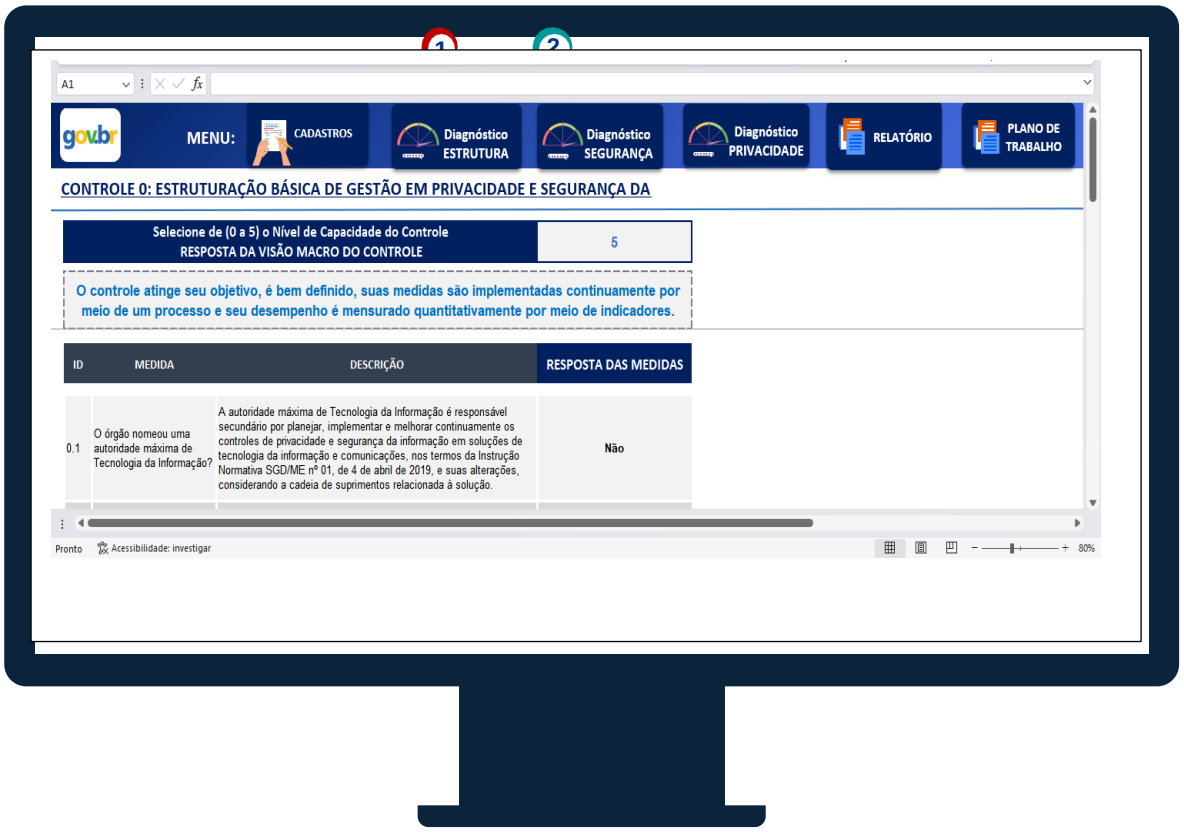
3. CADASTRO DO ÓRGÃO

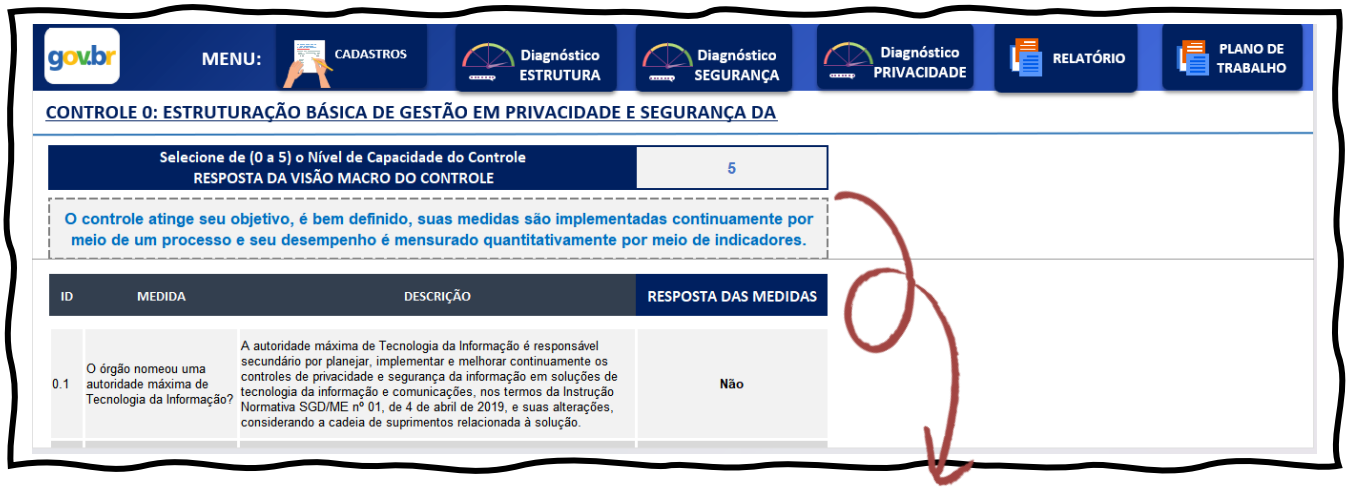
3.1 Adicionar Contatos



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.

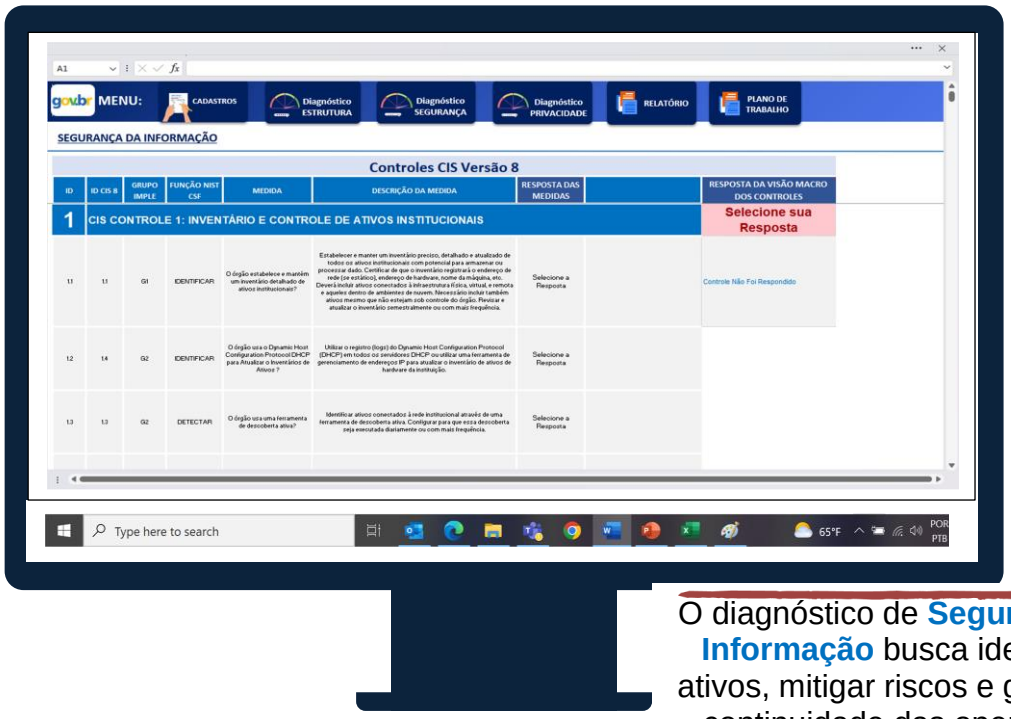
3.2 Estruturação básica de gestão em privacidade e segurança da informação



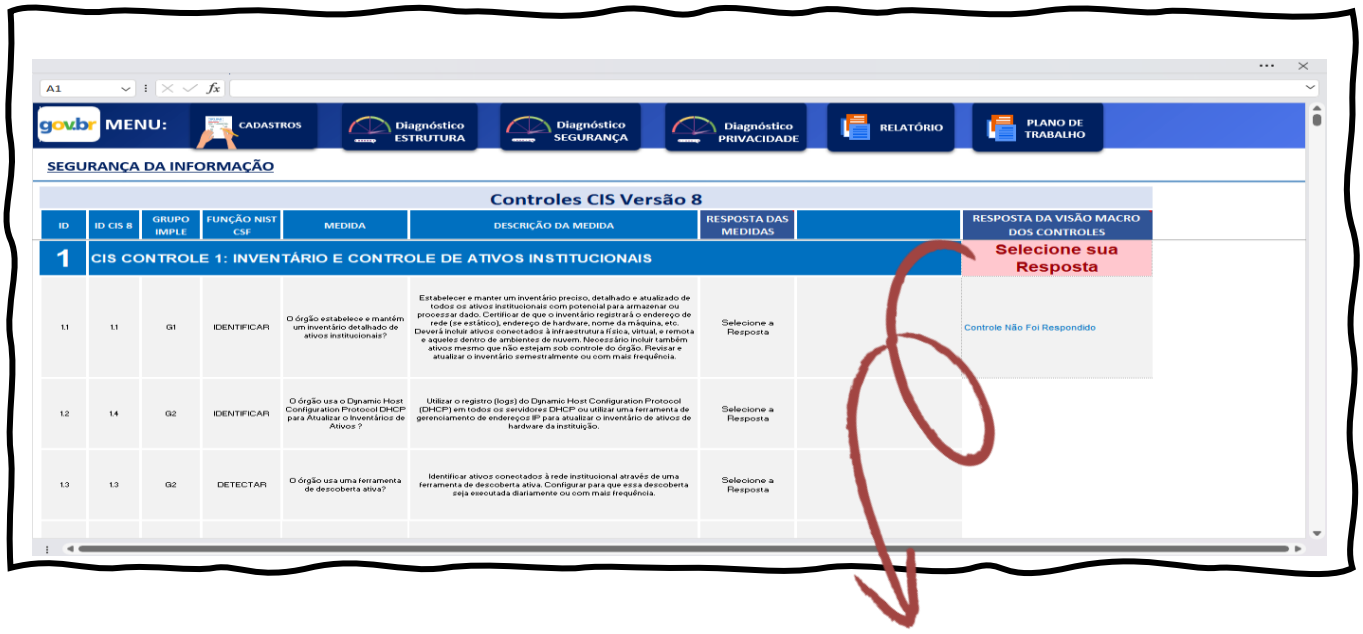


É imprescindível o preenchimento do nível de capacidade e de todas suas medidas.

3.3 Diagnóstico de Segurança da Informação



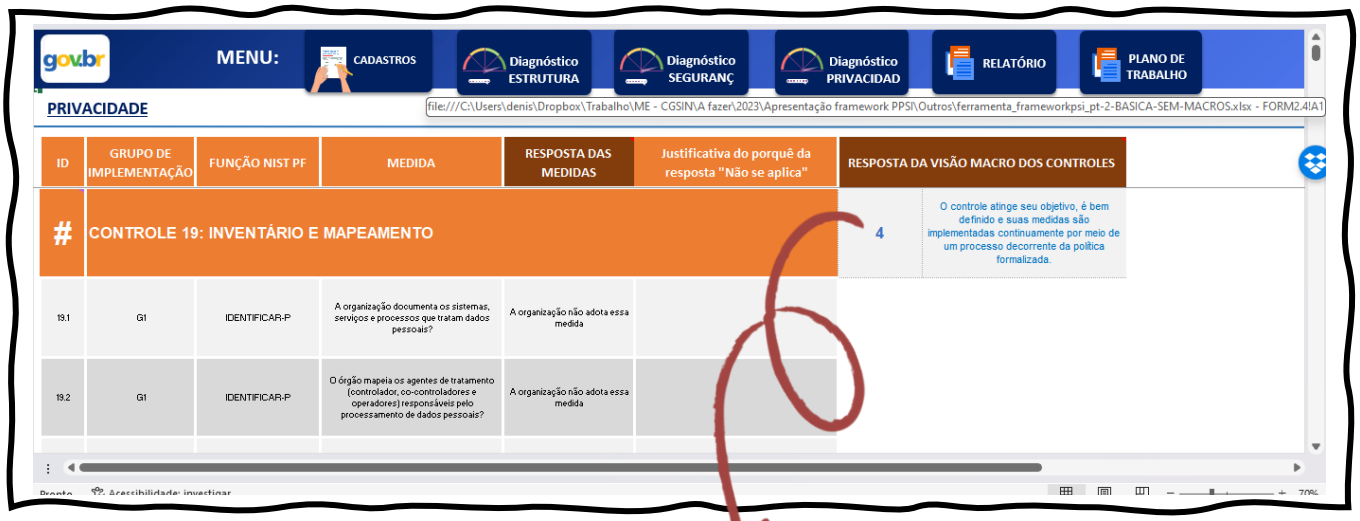
O diagnóstico de **Segurança da Informação** busca identificar ativos, mitigar riscos e garantir a continuidade das operações.



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

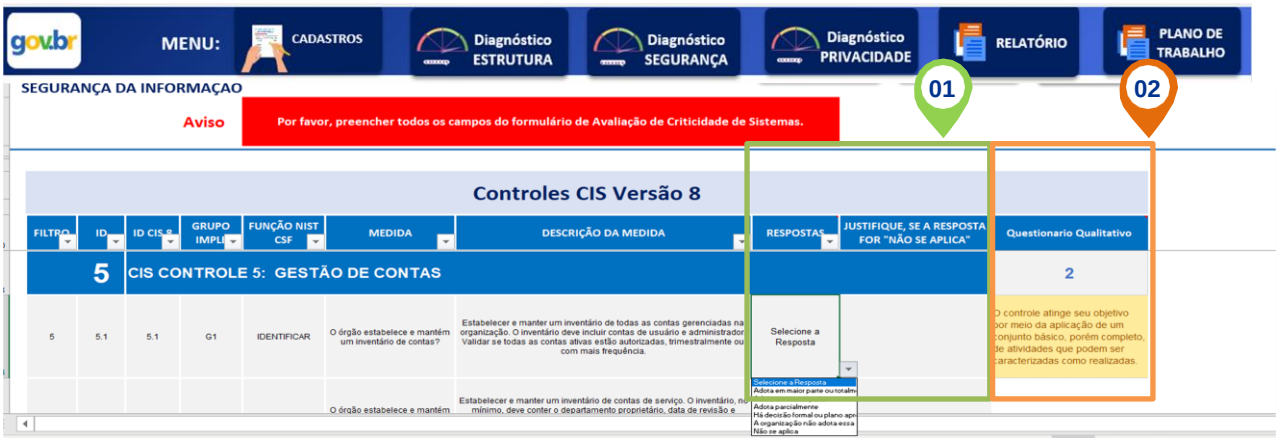
3.4 Diagnóstico de Privacidade

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

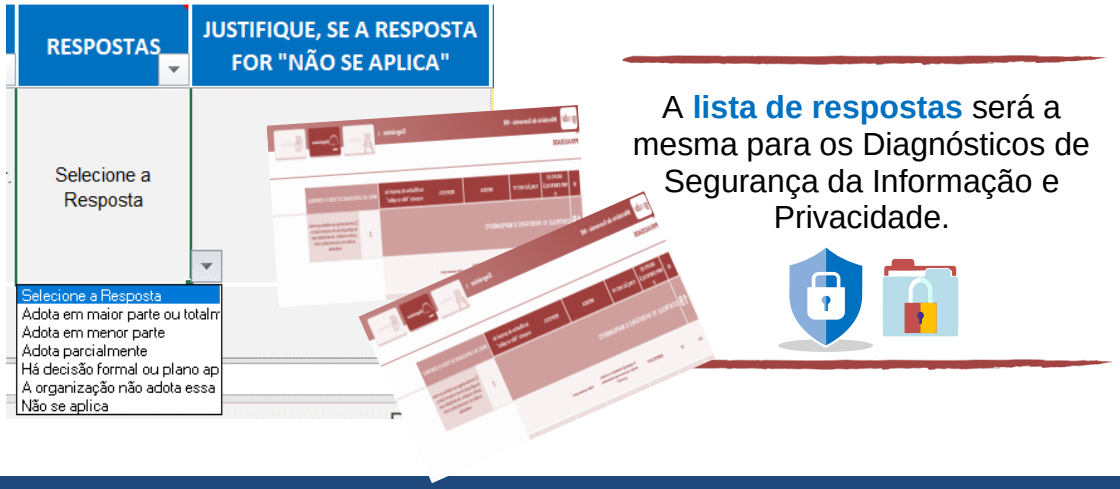


É imprescindível o preenchimento do nível de capacidade e de todas suas medidas.

3.5 Legenda da Lista de Opção de Resposta



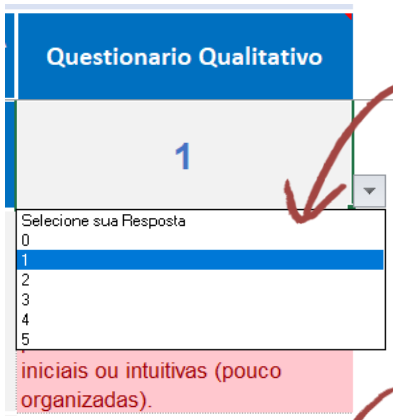
3.6 Lista de Respostas dos Diagnósticos de SI e Privacidade 01



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.

Há decisão formal ou plano aprovado para implementar	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.
A organização não adota essa medida	Não há qualquer decisão formal ou plano aprovado, tampouco implementação da medida.
Não se aplica	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



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.

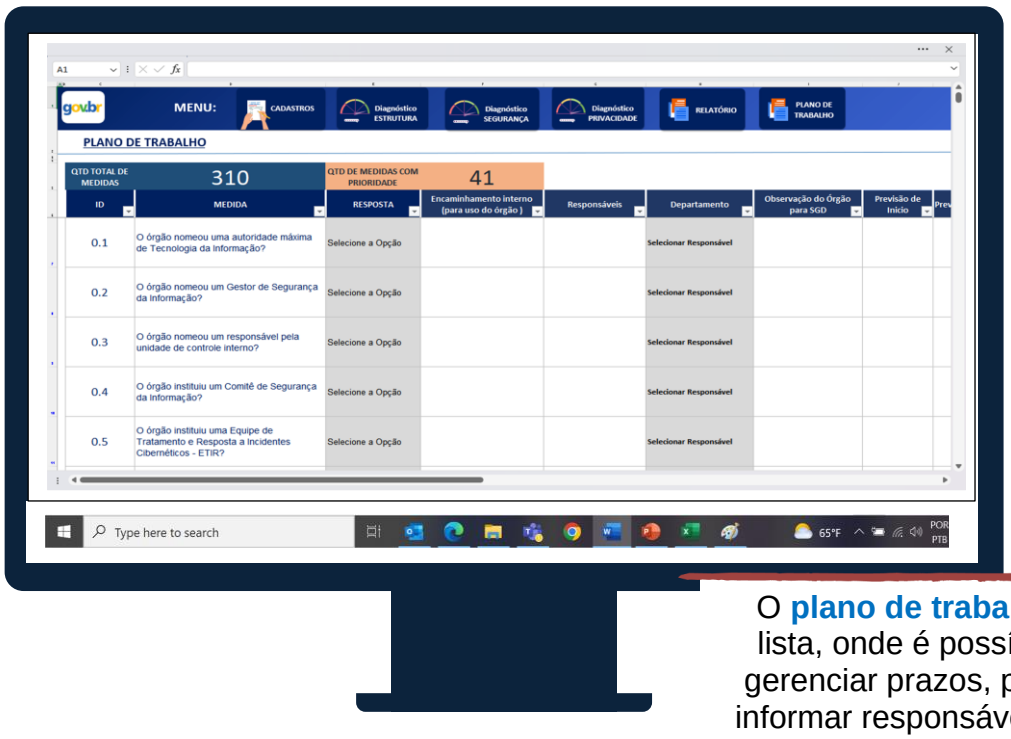
FIQUE ATENTO!

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

Planos de Trabalho

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



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

AVISO!!!

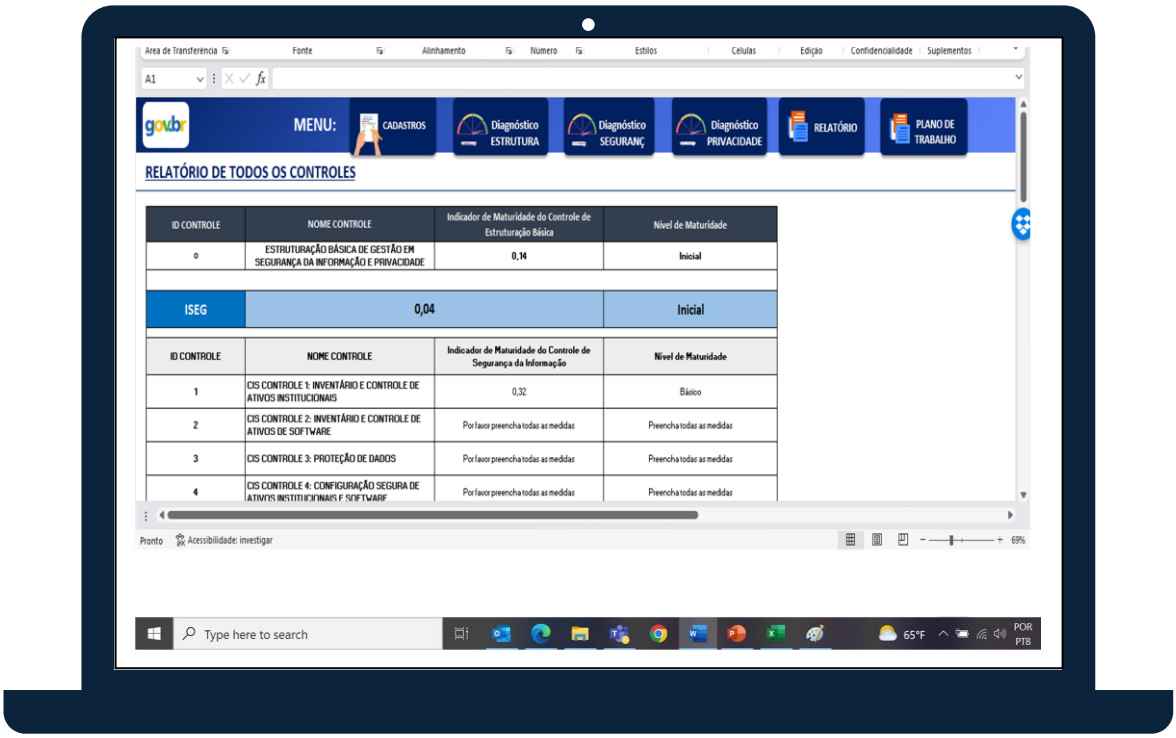
*Ao ter acesso ao formulário pela **primeira vez para avaliar** os planos de Trabalho é importante clicar no botão "**Planos de Trabalho**, e então preencher os demais campos do formulário do plano de Trabalho.*

3.8.1 *Descrição de cada coluna:*

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	**DEPARTAMENTO**	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	**OBSERVAÇÃO DO ÓRGÃO PARA SGD**	Serve para que o órgão possa inserir informação a respeito	É opcional o preenchimento desse campo.
8	**PREVISÃO DE INÍCIO**	Serve para direcionar para o responsável a data inicial do plano de trabalho.	É **imprescindível** que preencha a data de previsão de início do plano de trabalho
9	**PREVISÃO DE FIM**	Serve para direcionar para o responsável a data fim do plano de trabalho.	É **imprescindível** que preencha a data de previsão de fim do plano de trabalho para o funcionamento correto do preenchimento dos dados na ferramenta.
10	**STATUS PA**	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	**STATUS MEDIDA**	É um campo que permite controlar o a medida que foi finalizada e a que ainda não foi finalizada.	É **imprescindível** que selecione uma das duas opções (**finalizado** ou **não finalizado**) para controle do status do plano de trabalho e outros recursos da ferramenta.
12	**NOVA RESPOSTA**	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 significante.
13	**PRIORIDADE**	A lista com as opções de respostas “Sim” ou “Não”, possibilita ao respondente indicar se a medida é prioridade. **Todas as medidas do controle 0 serão prioridades**. 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



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

Telefone: (61) 2020-2046

DEPARTAMENTO DE
PRIVACIDADE E SEGURANÇA DA INFORMTRABALHO

SECRETARIA DE
GOVERNO DIGITAL

MINISTÉRIO DA
GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS