

Manual do Usuário da Ferramenta do Framework de Privacidade e Segurança da Informação - Ciclo 5

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

Versão 8.1

Brasília, Julho de 2025

MANUAL DO USUÁRIO DA FERRAMENTA DO FRAMEWORK DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO – CICLO 5

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 PRIVACIDADE

Marta Juvina de Medeiros

Coordenadora-Geral de Privacidade

COORDENAÇÃO-GERAL DE SEGURANÇA DA INFORMAÇÃO

Loriza Andrade Vaz de Melo

Coordenadora-Geral de Segurança da Informação

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

Carlos Mathias Mota Vargas

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

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)
10/01/2023	4.0	Quarta versão - Manual do Usuário Ferramenta (PPSI)
28/06/2024	5.0	Quinta versão - Manual do Usuário Ferramenta (PPSI)
21/11/2024	6.0	Sexta versão - Manual do Usuário Ferramenta (PPSI)
11/12/2024	7.0	Sétima versão - Manual do Usuário Ferramenta (PPSI)
18/06/2025	8.0	Oitava versão - Manual do Usuário Ferramenta (PPSI)
29/07/2025	8.1	Oitava primeira versão - Manual do Usuário Ferramenta (PPSI)

SUMÁRIO

AVISO INICIAL E EXPRESSÃO DE GRATIDÃO.....	ERRO! INDICADOR NÃO DEFINIDO.
1. INTRODUÇÃO.....	7
2. FERRAMENTA E ESTRUTURAÇÃO BÁSICA DE GESTÃO	8
3. CADASTRO DO ÓRGÃO	9
3.1 ADICIONAR CONTATOS	9
3.2 ESTRUTURAÇÃO BÁSICA DE GESTÃO EM PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO	10
3.3 DIAGNÓSTICO DE SEGURANÇA DA INFORMAÇÃO.....	11
3.4 DIAGNÓSTICO DE PRIVACIDADE	12
3.5 LEGENDA DA LISTA DE OPÇÃO DE RESPOSTA	13
3.6 LISTA DE RESPOSTAS DOS DIAGNÓSTICOS DE SI E PRIVACIDADE	13
3.7 LISTA DE RESPOSTAS QUALITATIVA.....	14
3.8 PLANOS DE TRABALHO.....	16
3.8.1 <i>Descrição de cada coluna:</i>	17
4. RELATÓRIOS.....	19
MENSAGEM FINAL	20

AVISO INICIAL E AGRADECIMENTOS

Este manual tem como objetivo orientar os usuários na utilização da **Ferramenta do Framework de Privacidade e Segurança da Informação (PPSI)**, versão 8.0, desenvolvida para o **Ciclo 5 do Programa de Privacidade e Segurança da Informação (PPSI)**.

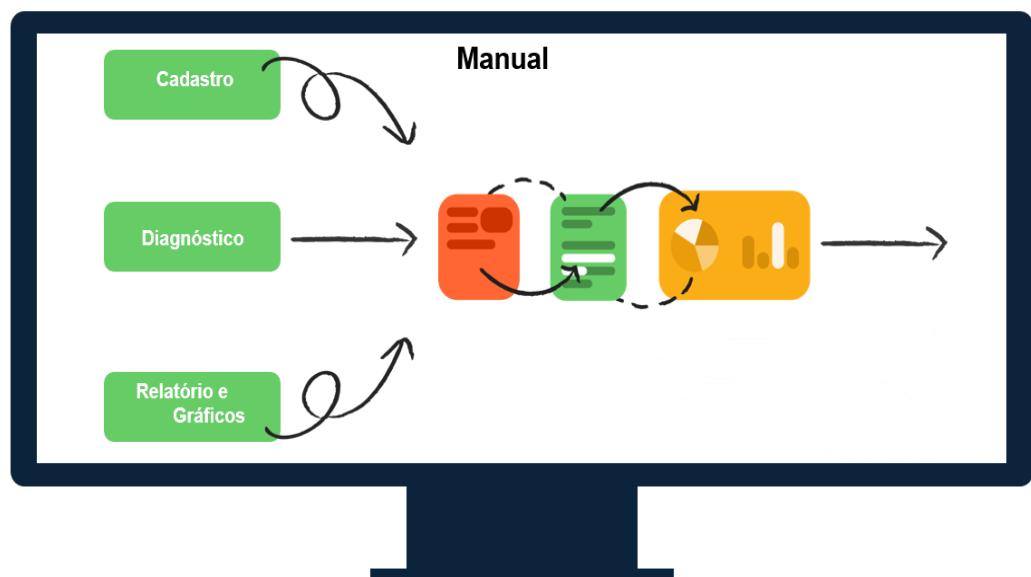
Agradecemos, de forma expressa, a todos os órgãos e entidades da **Administração Pública Federal (APF)** pela participação, comprometimento e empenho na aplicação desta ferramenta, contribuindo diretamente para o fortalecimento da **privacidade, proteção de dados e segurança da informação no setor público federal**.

 **Atenção:** a versão recomendada para utilização da ferramenta é o **Microsoft Excel 2019 ou superior**. Embora seja possível operá-la em versões anteriores, alertamos que **algumas fórmulas e funcionalidades podem não funcionar corretamente**, podendo impactar o preenchimento e o processamento dos dados.

1. INTRODUÇÃO

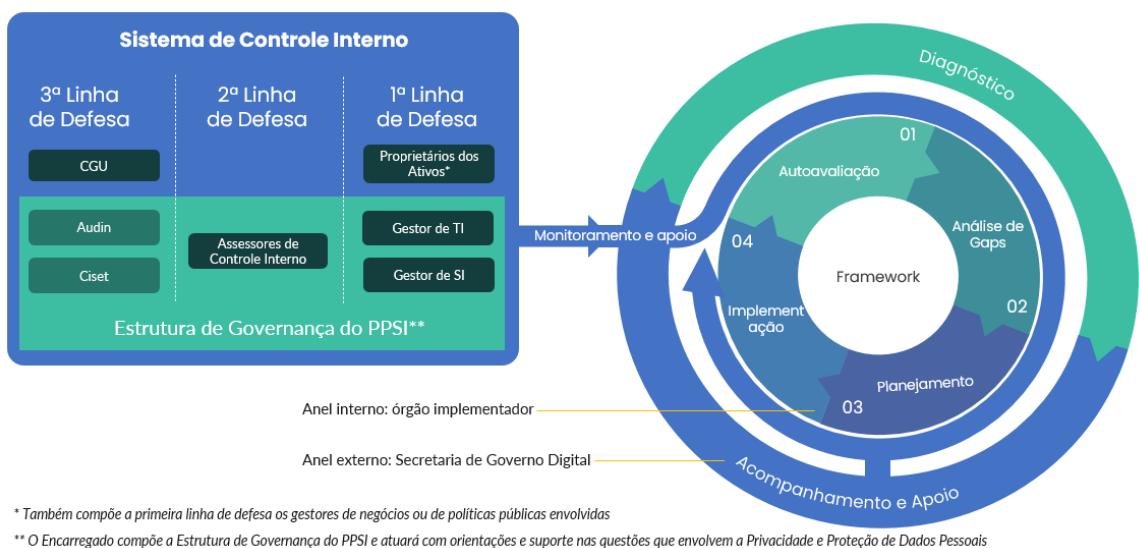
Seja bem-vindo ao **Manual do Usuário da Ferramenta do Framework de Privacidade e Segurança da Informação (PPSI)**, versão **8.0**, desenvolvida para o **Ciclo 5** do Programa de Privacidade e Segurança da Informação.

Este manual tem como objetivo **orientar os usuários no preenchimento, análise e utilização da ferramenta**, que é o instrumento central para o **diagnóstico, gestão e acompanhamento das práticas de privacidade e segurança da informação** nos órgãos da **Administração Pública Federal (APF)**.



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.



3. CADASTRO DO ÓRGÃO

3.1 Adicionar Contatos

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

ID	MEDIDA	DESCRÍÇÃO	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

ID	MEDIDA	DESCRÍÇÃO	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 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
19	CONTROLE 19: INVENTÁRIO E MAPEAMENTO					Selecione sua Resposta <small>Controle Não Foi Respondido</small>
19.1	G1	IDENTIFICAR-P	A organização documenta os sistemas, serviços e processos que tratam dados pessoais?	Selecione a Resposta		



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

3.5 Legenda da Lista de Opção de Resposta

Controles CIS Versão 8

5 CIS CONTROLE 5: GESTÃO DE CONTAS

O órgão estabelece e mantém um inventário de contas?

O órgão estabelece e mantém

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. Immediatamente ou com mais frequência.

Selecionar a Resposta

Selecionar a Resposta
Adota em maior parte ou totalmente
Adota em menor parte
Adota parcialmente
Há decisão formal ou plano ap...
A organização não adota essa...
Não se aplica

Justifique, se a resposta for "não se aplica"

O controle atinge seu objetivo por meio da aplicação de um conjunto básico, porém completo, de atividades que podem ser caracterizadas como realizadas.

3.6 Lista de Respostas dos Diagnósticos de SI e Privacidade

A **lista de respostas** terá o mesmo padrão 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.

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

02

Questionario Qualitativo

1

Seleciona 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.



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		178									
C.	V.	ID	MEDIDA	RESPOSTA	Encaminhamento Interno (uso do órgão)	Responsável	Departamento	Observação do Órgão SGD	Previsão Início	Previsão Fim	Status Plano de Ação	Status Medida	Prioridade	
1	0.1	O Órgão nomeou uma autoridade máxima de Tecnologia da Informação?	Selecionar a Opção			Selecionar Responsável					Atrasado	Não Finalizado	Sim	
1	0.2	O Órgão nomeou um Gestor de Segurança da Informação?	Selecionar a Opção			Selecionar Responsável					Atrasado	Não Finalizado	Sim	
1	0.3	O Órgão nomeou um responsável pela unidade de controle interno?	Selecionar a Opção			Selecionar Responsável					Atrasado	Não Finalizado	Sim	
1	0.4	O Órgão instituiu um Comitê de Segurança da Informação?	Selecionar a Opção			Selecionar Responsável					Atrasado	Não Finalizado	Sim	
1	0.5	O Órgão instituiu uma Equipe de Tratamento e Resposta a Incidentes Ciberneticos - ETIR?	Selecionar a Opção			Selecionar Responsável					Atrasado	Não Finalizado	Sim	

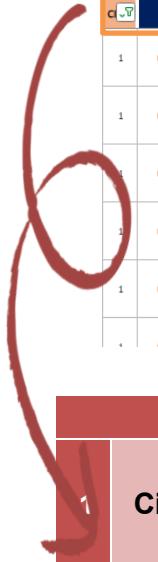


O **plano de trabalho** é uma lista, onde é possível criar e gerenciar prazos, prioridades, informar responsáveis e alterar respostas.

AVISO!!!

Ao ter acesso ao “**Plano de Trabalho** é fundamental conferir as medidas priorizadas para o Ciclo atual e os anteriores e então preencher os demais campos do formulário do Plano de Trabalho.
As medidas já priorizadas 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:



QTD TOTAL DE MEDIDAS		310	QTD DE MEDIDAS COM PRIORIDADE		178							
CICLO	ID	MEDIDA	RESPOSTA	Encaminhamento Interno (uso do órgão)	Responsável	Departamento	Observação do Órgão SGD	Previsão Início	Previsão Fim	Status PI de Ação	Status Medição	Prioridade
1	0.1	O órgão nomeou uma autoridade máxima de Tecnologia da Informação?	Selecionar a Opção			Selecionar Responsável				Atrasado	Não Finalizado	Sim
1	0.2	O órgão nomeou um Gestor de Segurança da Informação?	Selecionar a Opção			Selecionar Responsável				Atrasado	Não Finalizado	Sim
1	0.3	O órgão nomeou um responsável pela Unidade de controle interno?	Selecionar a Opção			Selecionar Responsável				Atrasado	Não Finalizado	Sim
1	0.4	O órgão instituiu um Comitê de Segurança da Informação?	Selecionar a Opção			Selecionar Responsável				Atrasado	Não Finalizado	Sim
1	0.5	O órgão instituiu uma Equipe de Tratamento e Resposta a Incidentes Cibéricos - ETIR?	Selecionar a Opção			Selecionar Responsável				Atrasado	Não Finalizado	Sim
1	0.6	O órgão elaborou uma Política de Segurança	Selecionar a Opção			Selecionar Responsável				Atrasado	Não Finalizado	Sim

COLUNA	DESCRÍÇÃO	RECOMENDAÇÃO
1 Ciclo	São os ciclos do plano	Pode ser utilizado para filtrar o ciclo atual.
2 ID	É o código identificador da medida	Não precisa de atuação do usuário final.
3 MEDIDA	Descrição da Medida	Não precisa de atuação do usuário final.
4 RESPOSTA	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 ENCAMINHAMENTO INTERNO	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 RESPONSÁVEL	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	DESCRÍÇÃO	RECOMENDAÇÃO
--------	-----------	--------------

7	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.
8	OBSERVAÇÃO DO ÓRGÃO PARA SGD	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	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 para as medidas priorizadas.
10	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 as medidas priorizadas.
11	STATUS PLANO DE AÇÃO	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	STATUS MEDIDA	É um campo que permite controlar a medida que foi finalizada e a que ainda não foi finalizada.	É imprescindível que seja selecionada uma das duas opções (finalizado ou não finalizado) para controle do status do plano de trabalho e outros recursos da ferramenta. Nesta versão essa coluna conta com uma automação que quando identifica a resposta “Sim” ou “Adota em maior parte ou totalmente” no diagnóstico, automaticamente preenche com “Finalizado”. Caso, por alguma razão, não preencha automaticamente, o órgão deve preencher.
13	PRIORIDADE	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.

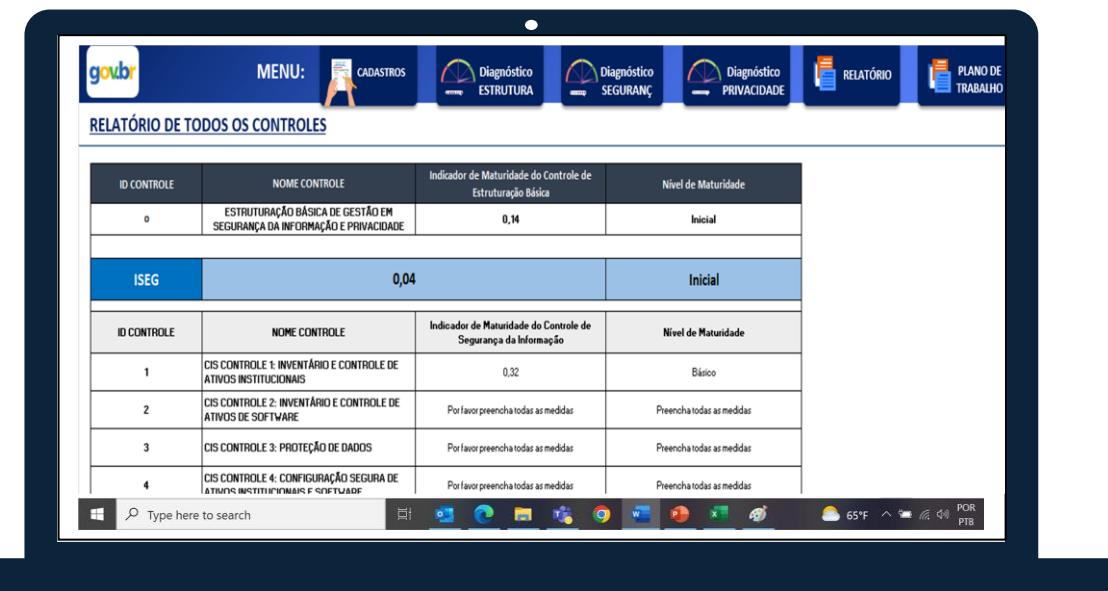
4. RELATÓRIOS

4.1 Análise dos Resultados

Após o preenchimento completo dos formulários, os indicadores serão automaticamente atualizadas com os resultados do órgão, incluindo:

- **Índice de Estruturação Básica:** Mede o nível de implementação estruturação.
- **Índice de Segurança (iSeg):** Mede a aderência aos controles de segurança.
- **Índice de Privacidade (iPriv):** Mede a aderência às práticas de privacidade.

Os painéis permitem uma análise visual da situação atual, a identificação de pontos fracos e o acompanhamento da evolução ao longo do tempo.



AVISO!!! *e 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 e a **Ferramenta do Framework v8.0** são guias valiosos para os órgãos e entidades da Administração Pública Federal.

Estamos empenhados em evoluir junto com os avanços tecnológicos e as mudanças regulatórias. Desejamos sucesso em suas jornadas e esforços para construir um ambiente digital cada vez mais seguro e respeitoso neste **Ciclo 5**.

**Dúvida?
Entre em
contato
conosco.**

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

Email: 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