Manual do Usuário da Ferramenta do Framework de Privacidade e Segurança da Informação

PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO (PPSI)

Versão 1.0

Brasília, novembro de 2022

MANUAL DO USUÁRIO DA FERRAMENTA DO FRAMEWORK DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

MINISTÉRIO DA ECONOMIA

Paulo Roberto Nunes Guedes

Ministro

SECRETARIA ESPECIAL DE DESBUROCRATIZAÇÃO, GESTÃO E GOVERNO DIGITAL

Leonardo José Mattos Sultani

Secretário Especial de Desburocratização, Gestão e Governo Digital

SECRETARIA DE GOVERNO DIGITAL

Fernando André Coelho Mitkiewicz

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

Flavia Patrícia Donata Vieira

Heráclito Ricardo Ferreira Gomes

Julierme Rodrigues da Silva

Marcus Paulo Barbosa Vasconcelos

Rogério Vinícius Matos Rocha

Romário César de Almeida
Sumaid Andrade de Albuquerque
Valdecy Oliveira de Araújo
Yuri Arcanjo De Carvalho

Histórico de Versões

Data	Versão	Descrição	Autor
04/11/2022	1.0	Primeira versão do Manual do Usuário Ferramenta (PPSI)	Equipe Técnica de Elaboração

SUMÁRIO

AVISO PRELIMINAR E AGRADECIMENTOS

O presente manual tem como finalidade orientar os usuários na utilização das funcionalidades da **Ferramenta do Framework de Privacidade e Segurança da Informação**[1] na versão 1.0, contendo as instruções necessárias para melhor aproveitamento de suas funções. O documento é especialmente recomendado e dirigido aos órgãos e às entidades da Administração Pública Federal - APF para orientar a aplicabilidade da ferramenta, auxiliando no preenchimento das respostas aos diagnósticos, o que não impede de ser utilizado por outras instituições que busquem orientações sobre o tema.

Cumpre reconhecer a fundamental parceria com o Governo do Reino Unido, no âmbito do Programa de Acesso Digital, que viabilizou o desenvolvimento da ferramenta, descrita neste manual, para aplicação do framework proposto.

Nesse cenário, a Secretaria de Governo Digital enfatiza que:

a) não representa, tampouco se manifesta em nome da Embaixada Britânica;

b) não assume nenhuma responsabilidade administrativa, técnica ou jurídica pelo uso ou pela interpretação inadequados, fragmentados ou parciais do presente **Manual**.

[1] Disponível em:
Versão para Office 365 em português: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/ferramenta_frameworkpsi_pt-2.xlsm
Versão para Office 365 em inglês: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/ferramenta_frameworkpsi_en-1.xlsm

1. INTRODUÇÃO

O **Manual do Usuário da Ferramenta do Framework de Privacidade e Segurança da Informação** orienta o uso da ferramenta citada pelo capítulo 7 do **Guia do Framework de Privacidade e Segurança da Informação**[2], o qual faz parte da série de guias operacionais[3] elaborados pela Secretaria de Governo Digital (SGD), da Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia para fomentar a privacidade, a proteção de dados pessoais e a segurança da informação[4].

O presente manual tem como finalidade orientar os usuários na utilização das funcionalidades da ferramenta versão 1.0, contendo as instruções necessárias para melhor aproveitamento de suas funções.

Este Manual será revisto e atualizado sempre que se fizer necessária a inclusão de ajustes na ferramenta para acompanhar o amadurecimento dos processos de privacidade e segurança da informação, bem como para alinhamento ao **Guia do Framework de Privacidade e Segurança da Informação.**

ORIENTAÇÕES IMPORTANTES:

A **Ferramenta do Framework de Privacidade e Segurança da Informação (Excel) possui macro**, ou seja, nada mais é que uma sequência de comandos e funções armazenados em um módulo de VBA.

Sugerimos que ao utilizar a ferramenta, verificar se no **pacote office 365** do órgão está habilitada a opção de macro, caso não esteja, é importante **consultar a TI se pode ser habilitada,** para saber como **habilitar** consulte o Anexo I deste manual. Ademais, para o perfeito funcionamento da macro é preciso utilizar o Excel na **versão desktop**.

Cabe ressaltar que ao utilizar a **Ferramenta do Framework de Privacidade e Segurança da Informação** é imprescindível a utilização da versão aplicável ao idioma do pacote office 365 instalado na máquina onde será utilizado.

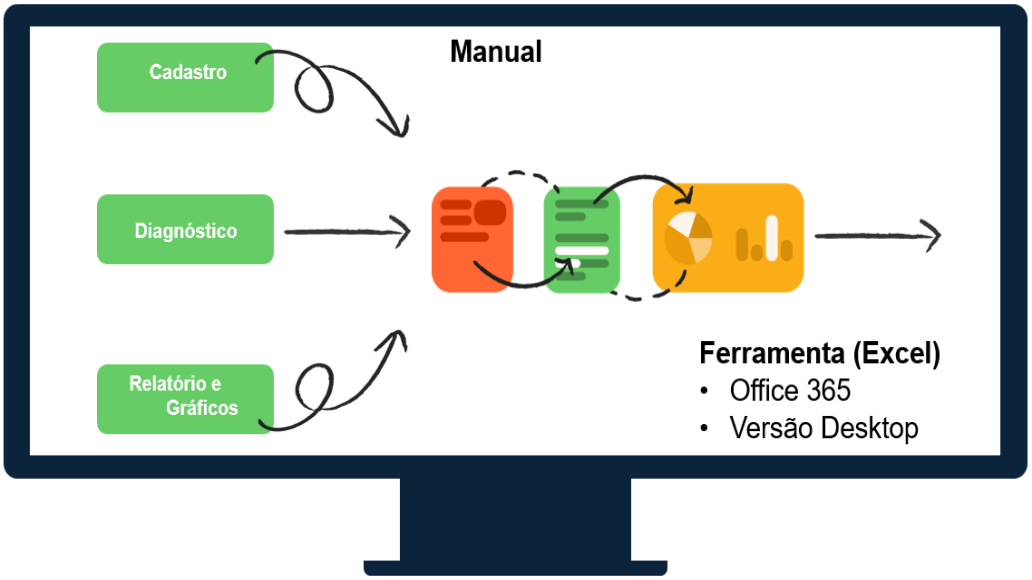
---

[2] Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias-operacionais-para-adequacao-a-lei-geral-de-protecao-de-dados-pessoais-lgpd

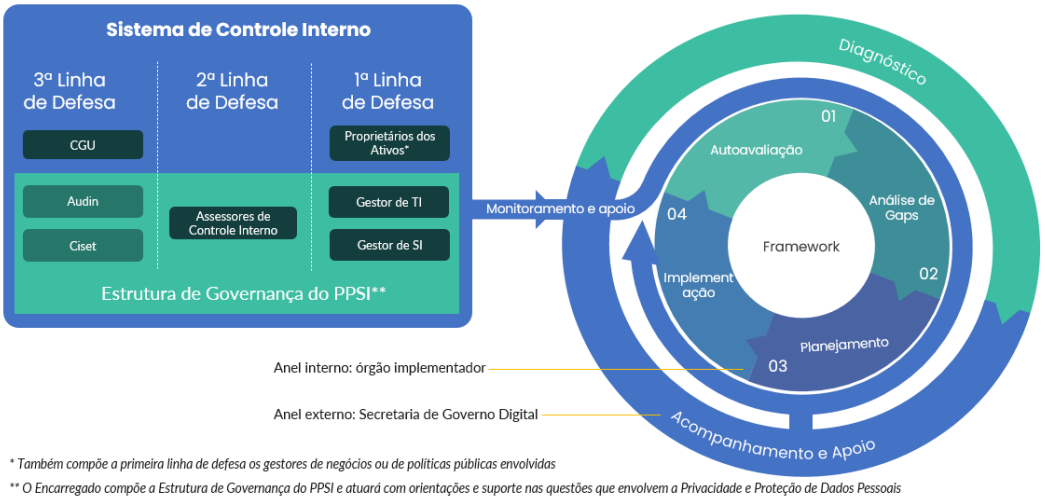
[3] Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias-operacionais-para-adequacao-a-lei-geral-de-protecao-de-dados-pessoais-lgpd

[4] Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

2. FERRAMENTA E ESTRUTURAÇÃO BÁSICA DE GESTÃO

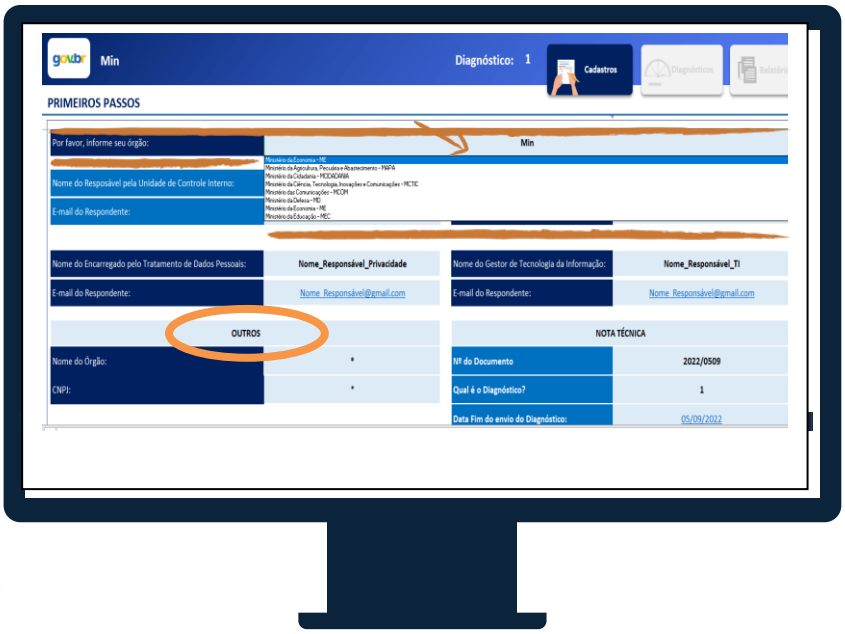


A ferramenta foi criada para ser utilizada na versão atual do office (Office 365 Versão Desktop). A Figura abaixo resume a metodologia de implementação a ser empregada na aplicação do Framework mostrando como estão relacionados o Sistema de Controle Interno (SCI) com os principais atores e as atividades a serem executadas.



3. CADASTRO DO ÓRGÃO

3.1 Adicionar o Nome do Órgão



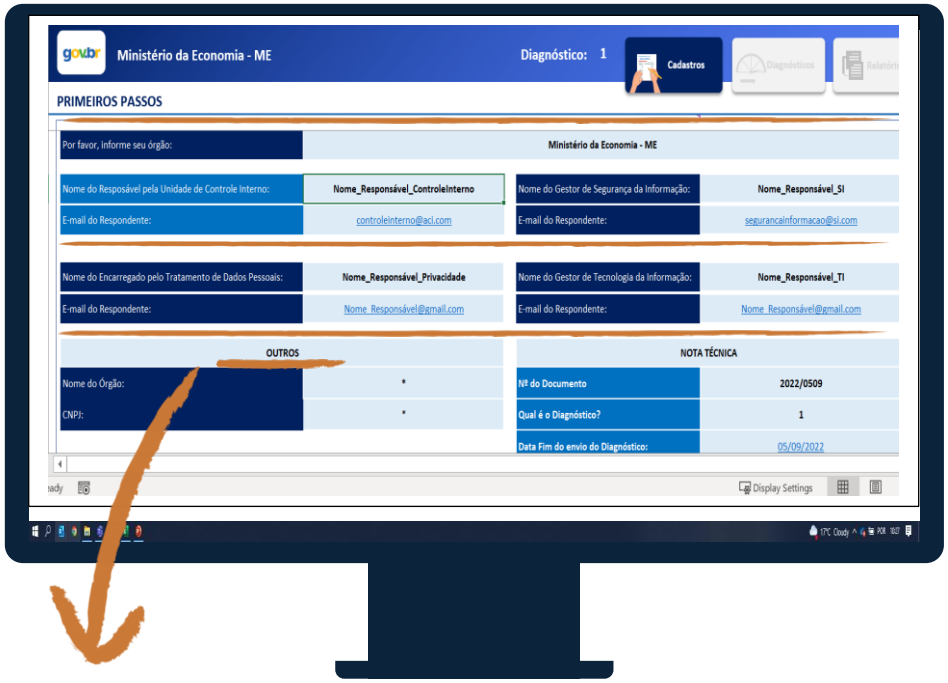
Nome do Órgão

Há possibilidade de pesquisar o nome do órgão respondente, ou se preferir é possível apagar toda informação do campo e pesquisar direto na lista

O nome do órgão em que trabalho **não está** na **lista**, **o que devo fazer**?

Procure a opção “**Outros**” na lista de Órgãos, selecione o campo e depois preencha os dados do nome do órgão e o CNPJ

3.2 Adicionar Contatos dos Respondentes



A opção “**Outros**” possibilitará inserir as informações de nome e e-mail para que a SGD possa entrar em contato com os responsáveis do preenchimento dos diagnósticos.

Nome do Resposável pela Unidade de Controle Interno:	Nome_Responsável_ControleInterno	Nome do Gestor de Segurança da Informação:	Nome_Responsável_SI
E-mail do Respondente:	controleinterno@aci.com	E-mail do Respondente:	segurancainformacao@si.com
Nome do Encarregado pelo Tratamento de Dados Pessoais:	Nome_Responsável_Privacidade	Nome do Gestor de Tecnologia da Informação:	Nome_Responsável_TI
E-mail do Respondente:	Nome_Responsável@gmail.com	E-mail do Respondente:	Nome_Responsável@gmail.com

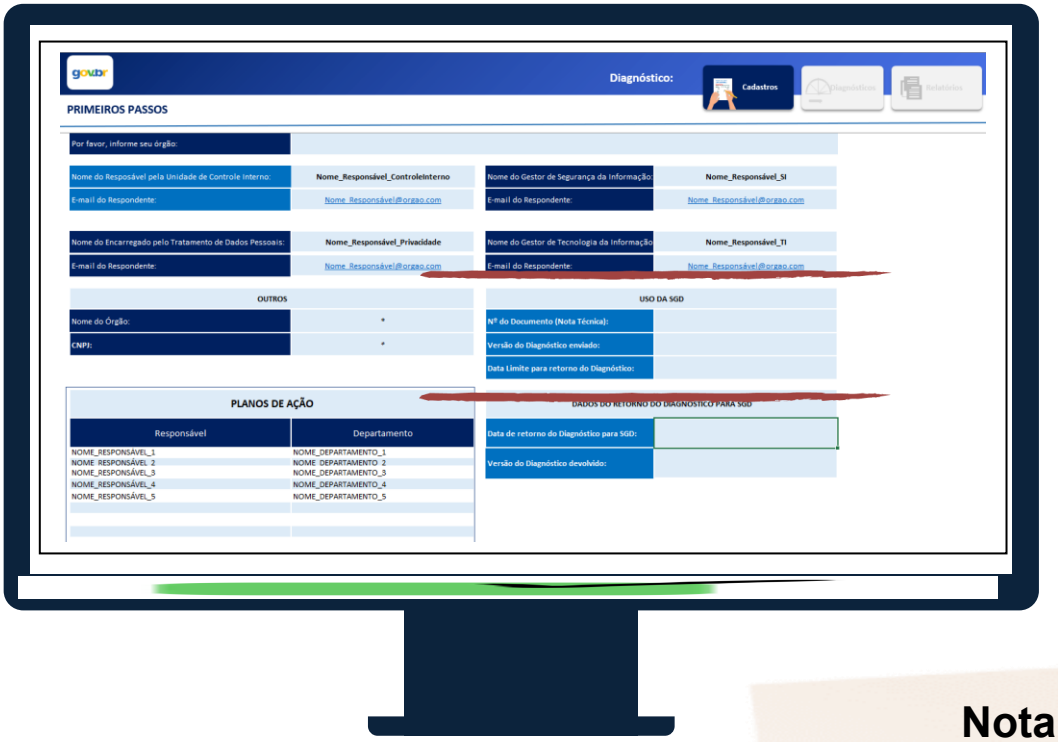
3.3 Adicionar Cadastro do responsável/Departamento dos Planos de Ação

O preenchimento dos nomes dos **responsáveis** e de seus respectivos departamentos permitirão que as **informações inseridas no cadastro** possam **aparecer no formulário dos planos de ação**, facilitando assim o preenchimento de quem ficará responsável por cada atividade dentro do plano de ação.

PLANOS DE AÇÃO

Responsável	Departamento
NOME_RESPONSÁVEL_1	NOME_DEPARTAMENTO_1
NOME_RESPONSÁVEL_2	NOME_DEPARTAMENTO_2
NOME_RESPONSÁVEL_3	NOME_DEPARTAMENTO_3
NOME_RESPONSÁVEL_4	NOME_DEPARTAMENTO_4
NOME_RESPONSÁVEL_5	NOME_DEPARTAMENTO_5

3.4 Nota Técnica



Nota Técnica

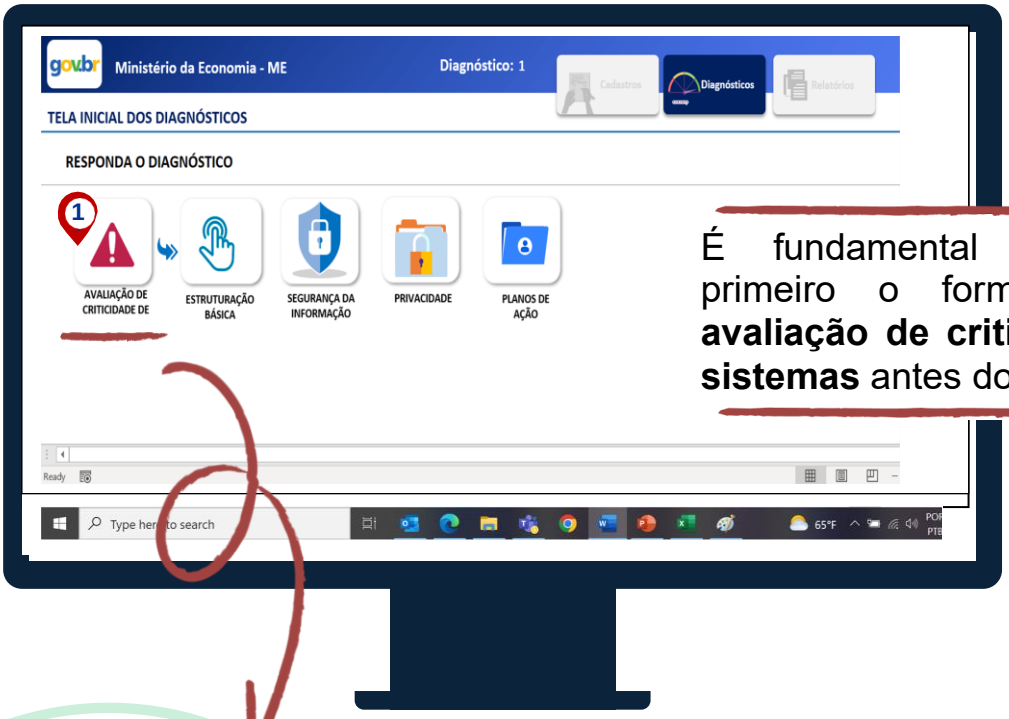
Todos os campos (número do documento, diagnóstico e a data final de envio) serão preenchidos pela SGD de acordo com a nota técnica.

Nota Técnica

A nota técnica, no contexto dessa ferramenta, é uma publicação oficial que reúne informações com orientações sobre os controles de segurança e privacidade que precisam ser priorizados.

4. DIAGNÓSTICO

4.1 Avaliação de Criticidade de Sistemas



É fundamental preencher primeiro o formulário **de avaliação de criticidade de sistemas** antes dos demais.

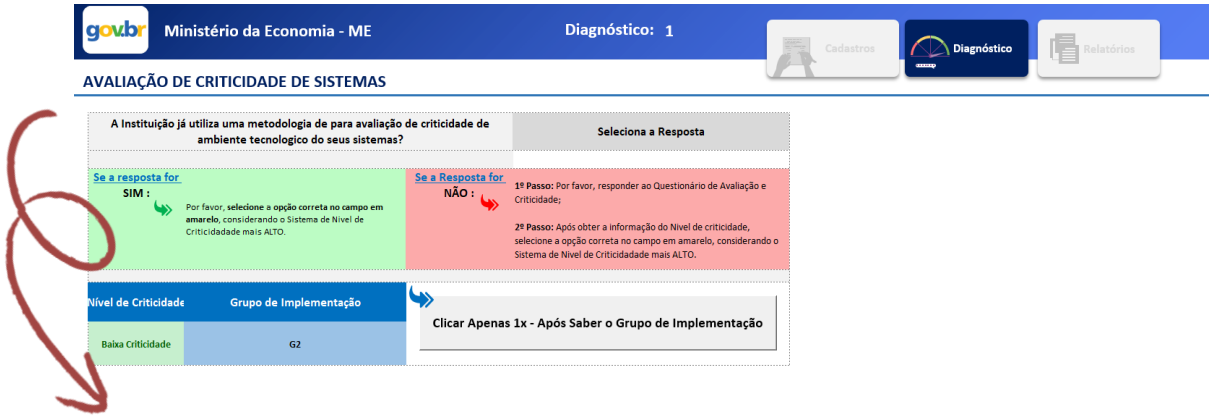
Avaliação de Criticidade de Sistemas

Ponto de partida para o diagnóstico. Tem por finalidade identificar o grupo de implementação a partir da informação do nível de criticidade do sistema mais crítico.

AVISO!!!

*Com a finalidade de facilitar a **avaliação de criticidade dos sistemas** relevantes, a SGD disponibiliza a título de sugestão para aqueles órgãos que não possuam uma metodologia própria, uma ferramenta em formato de planilha. A ferramenta pode ser encontrada no link:*

https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias-operacionais-para-adequacao-a-lei-geral-de-protecao-de-dados-pessoais-lgpd



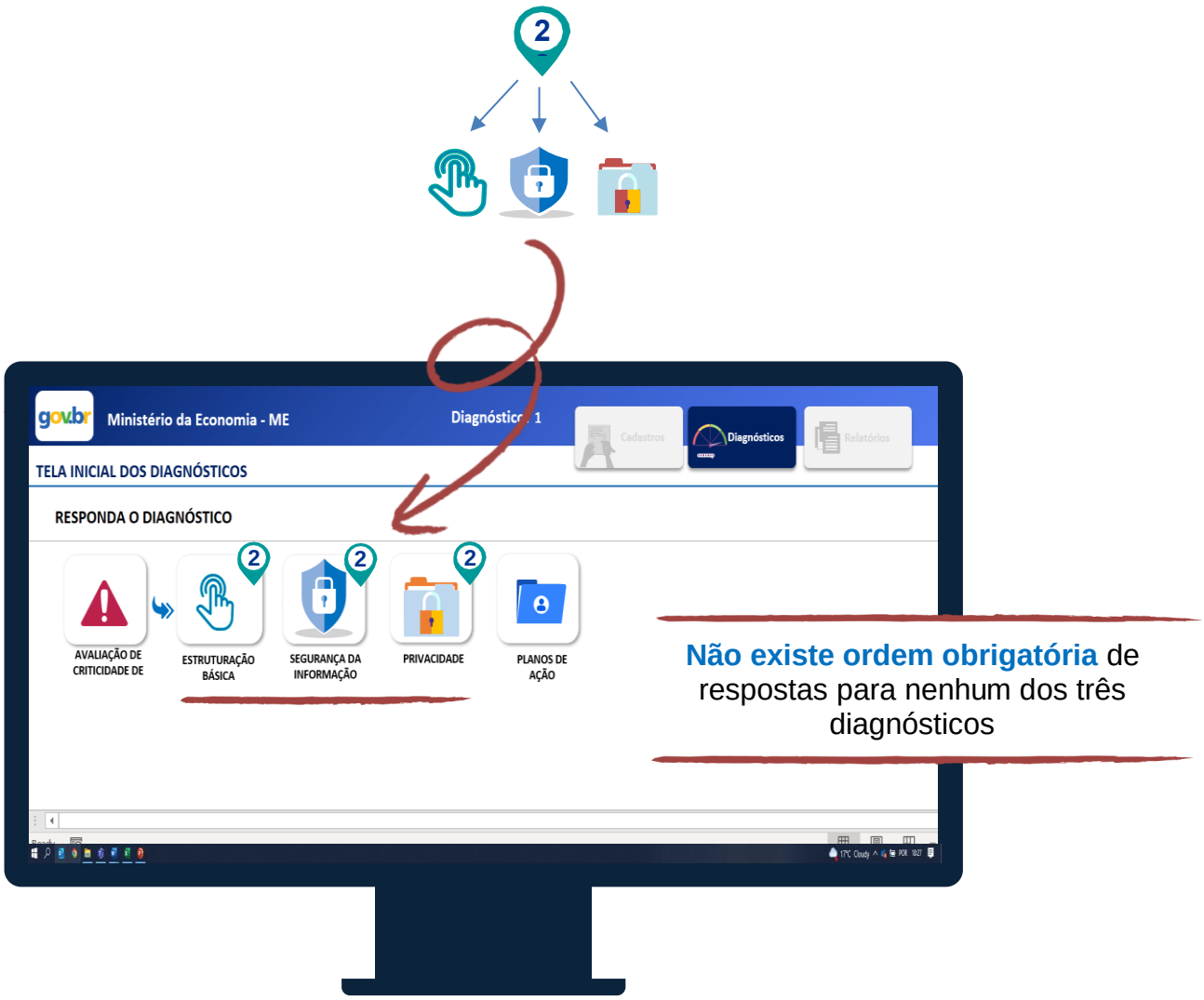
Esse formulário é o primeiro a ser preenchido.

Selecione a resposta e siga as orientações de acordo com o que foi respondido (caixa VERDE ou VERMELHA). O nível de criticidade deve ser selecionado de acordo com a criticidade do sistema relevante mais crítico selecionado pelo órgão, essa informação definirá o Grupo de implementação em que o órgão se enquadra, determinando os controles e medidas de segurança da informação e privacidade que serão de implementação obrigatória.

Aviso!!!

Após selecionar a criticidade e saber o grupo de implementação, é imprescindível clicar no botão abaixo. Ele preparará os diagnósticos de Segurança e Privacidade de acordo com o nível de implementação encontrado, eliminando das opções de respostas a opção “Não se aplica”, o que tornam essas medidas obrigatórias.

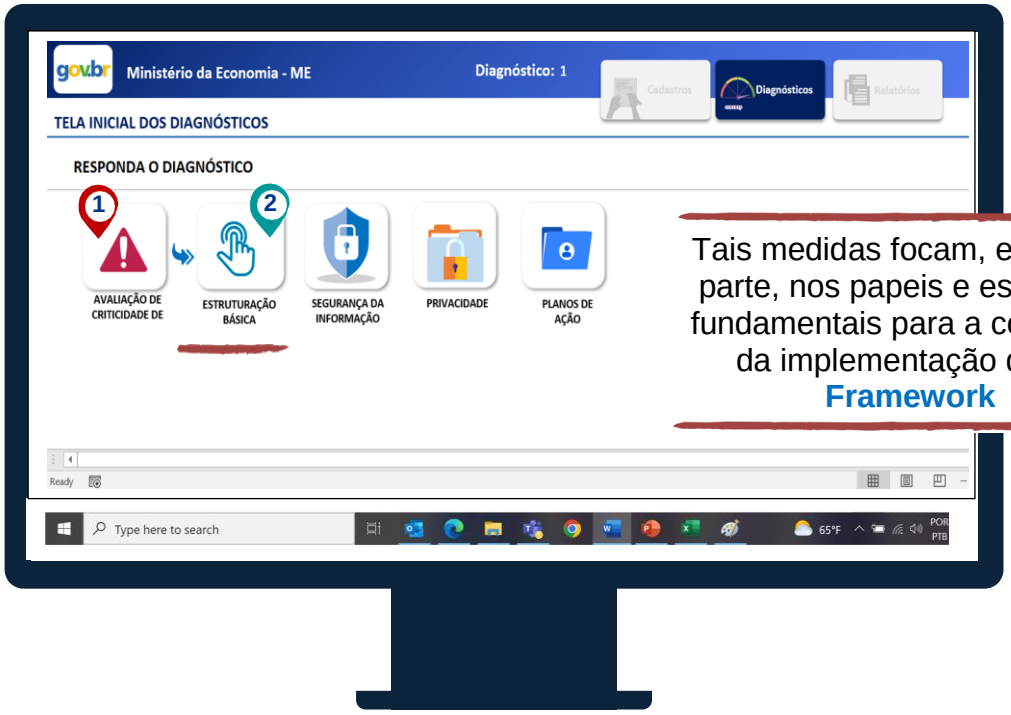
4.2 Diagnósticos de Estruturação básica, Diagnóstico de Segurança da Informação e Privacidade.



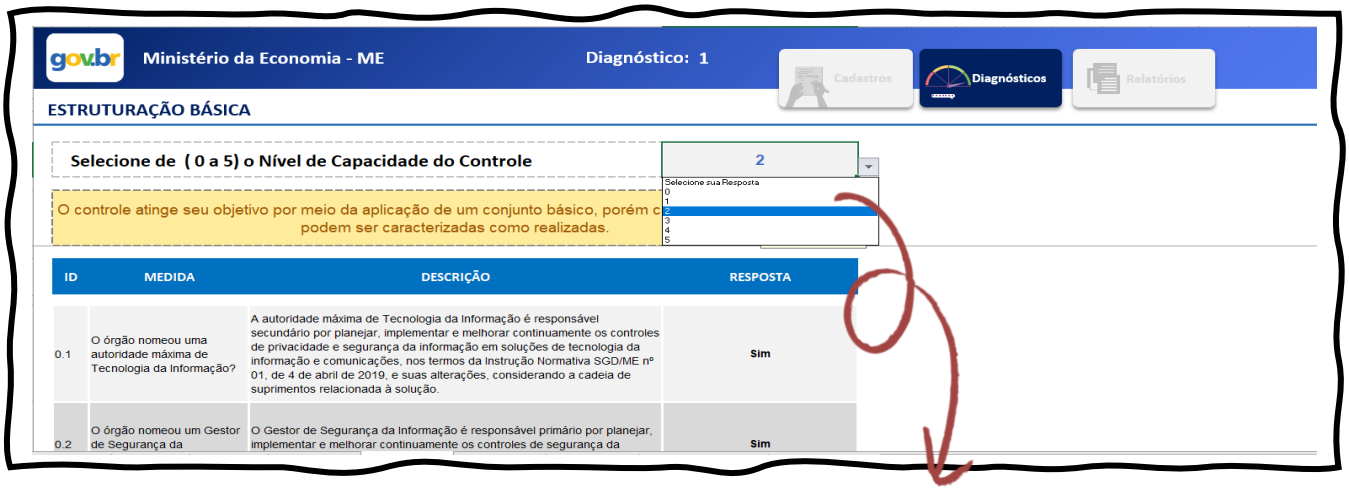
Estruturação Básica

Visa atender às ações específicas de conformidade básica estabelecidas na IN SGD/ME nº 01, de 4 de abril de 2019, IN CGU nº 3, de 9 de junho de 2017, IN GSI/PR nº 1, de 27 de maio de 2020 e LGPD - Lei nº 13.709, de 14 de agosto de 2018.

4.3 Estruturação básica de gestão em privacidade e segurança da informação

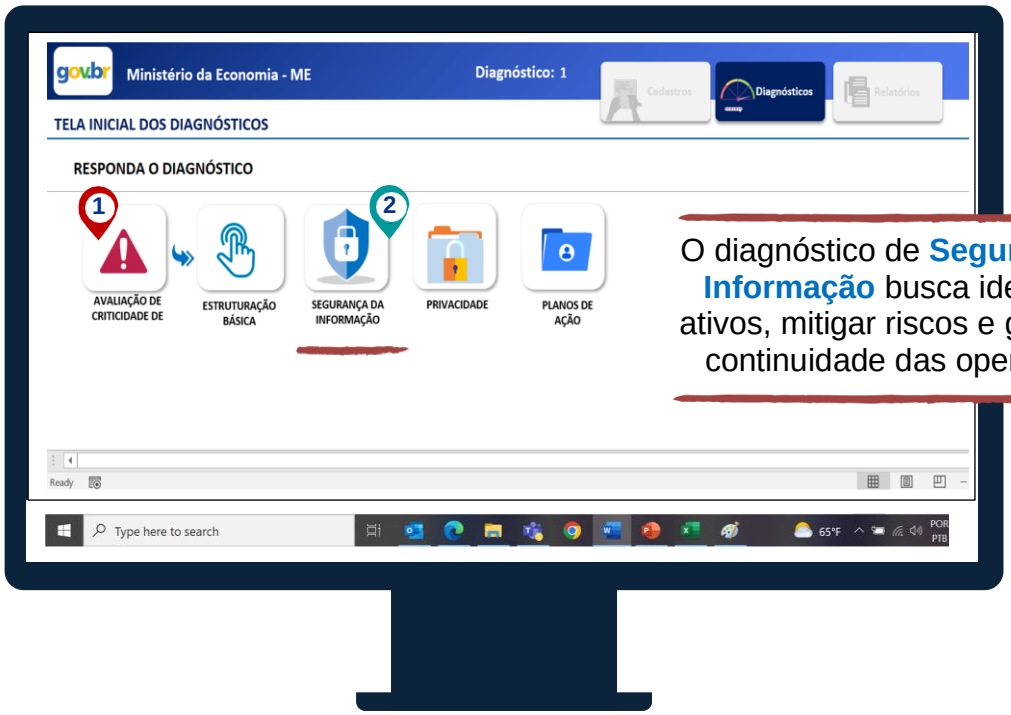


Tais medidas focam, em maior parte, nos papeis e estruturas fundamentais para a condução da implementação deste **Framework**

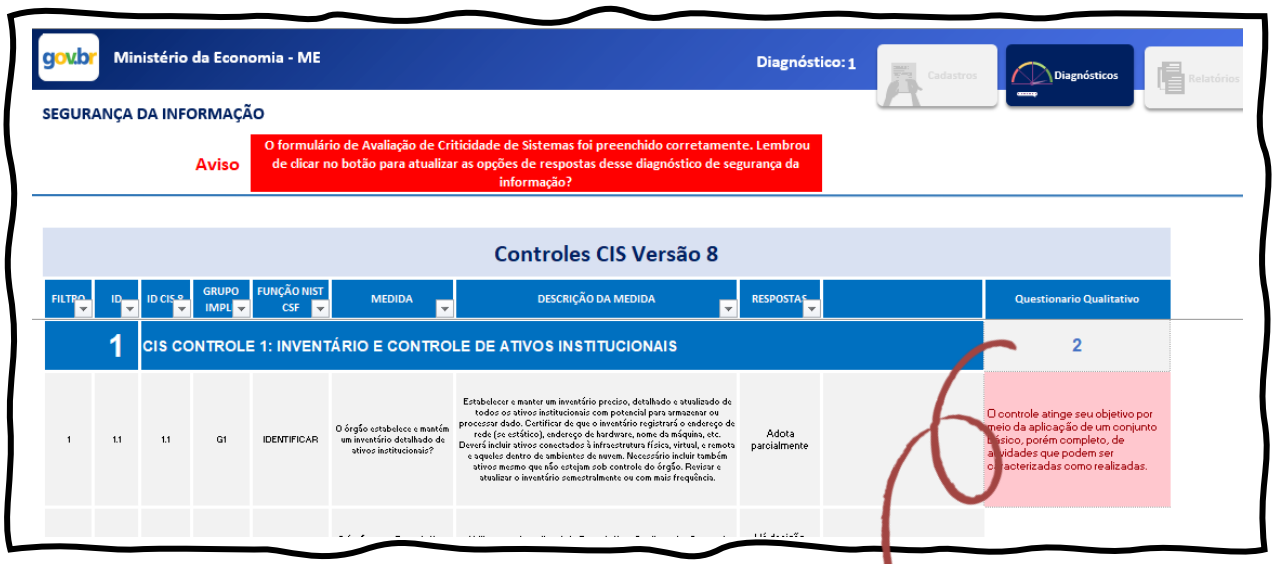


É imprescindível o preenchimento do nível de capacidade e de todas suas medidas.

4.4 Diagnóstico de Segurança da Informação

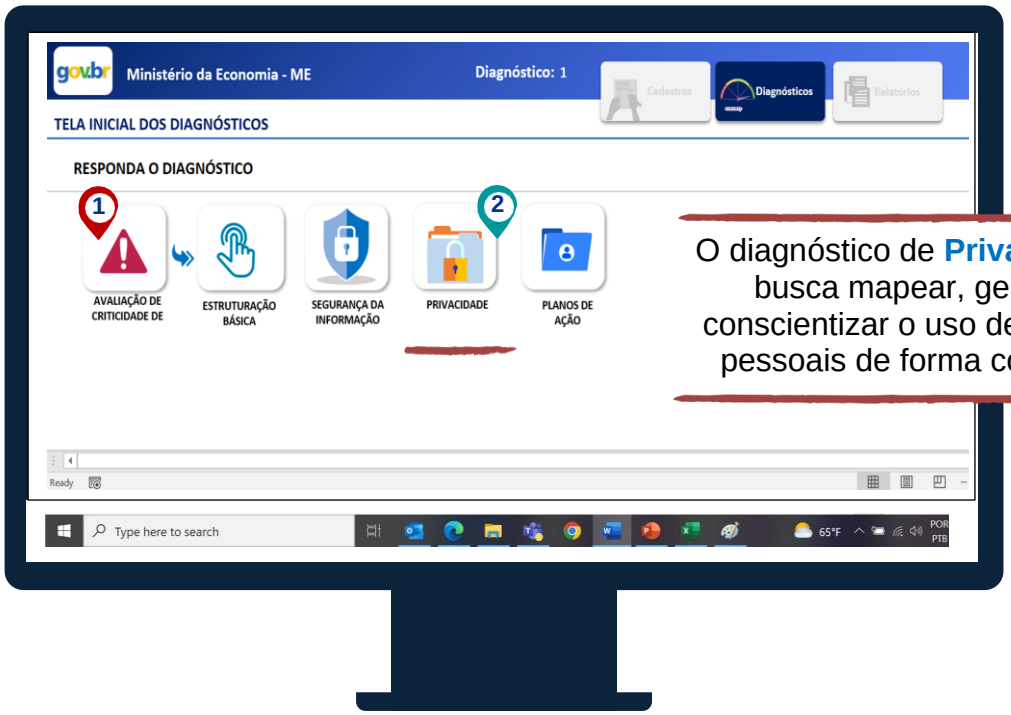


O diagnóstico de **Segurança da Informação** busca identificar ativos, mitigar riscos e garantir a continuidade das operações.



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

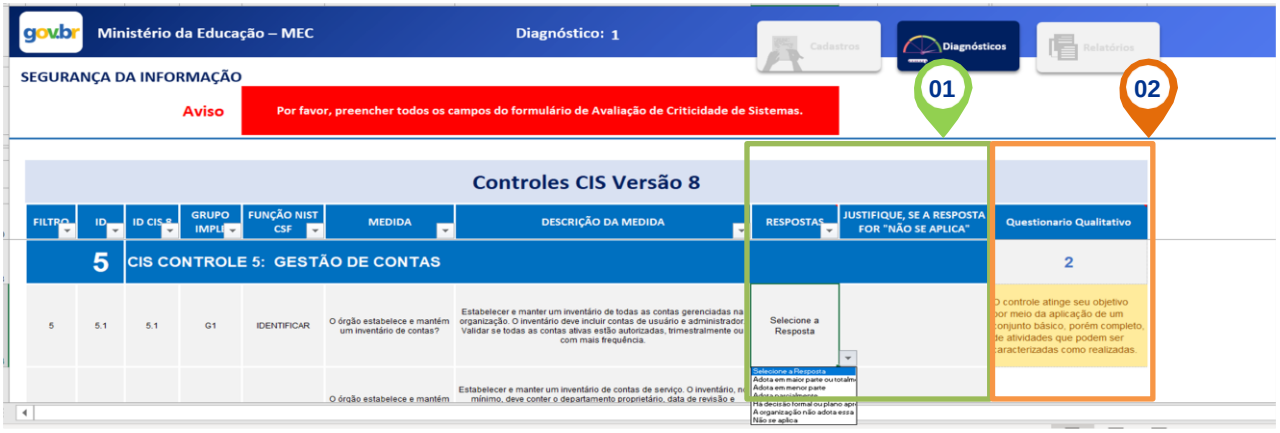
4.5 Diagnóstico de Privacidade



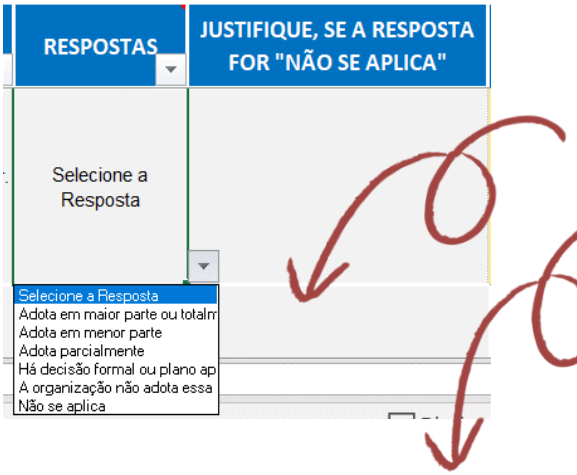
O diagnóstico de **Privacidade** busca mapear, gerir e conscientizar o uso de dados pessoais de forma correta.

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

4.6 Legenda da Lista de Opção de Resposta



4.7 Lista de Respostas dos Diagnósticos de SI e Privacidade 01

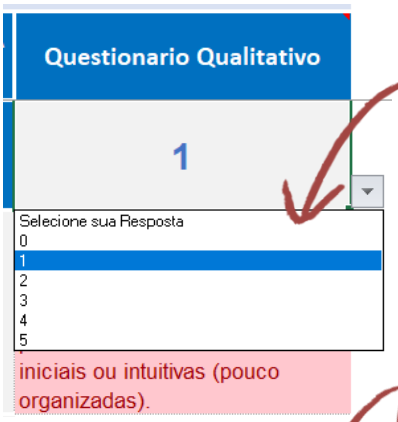


A **lista de respostas** será a mesma para os Diagnósticos de Segurança da Informação e Privacidade.

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.
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.

4.8 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 aplicação 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 aplicação 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.

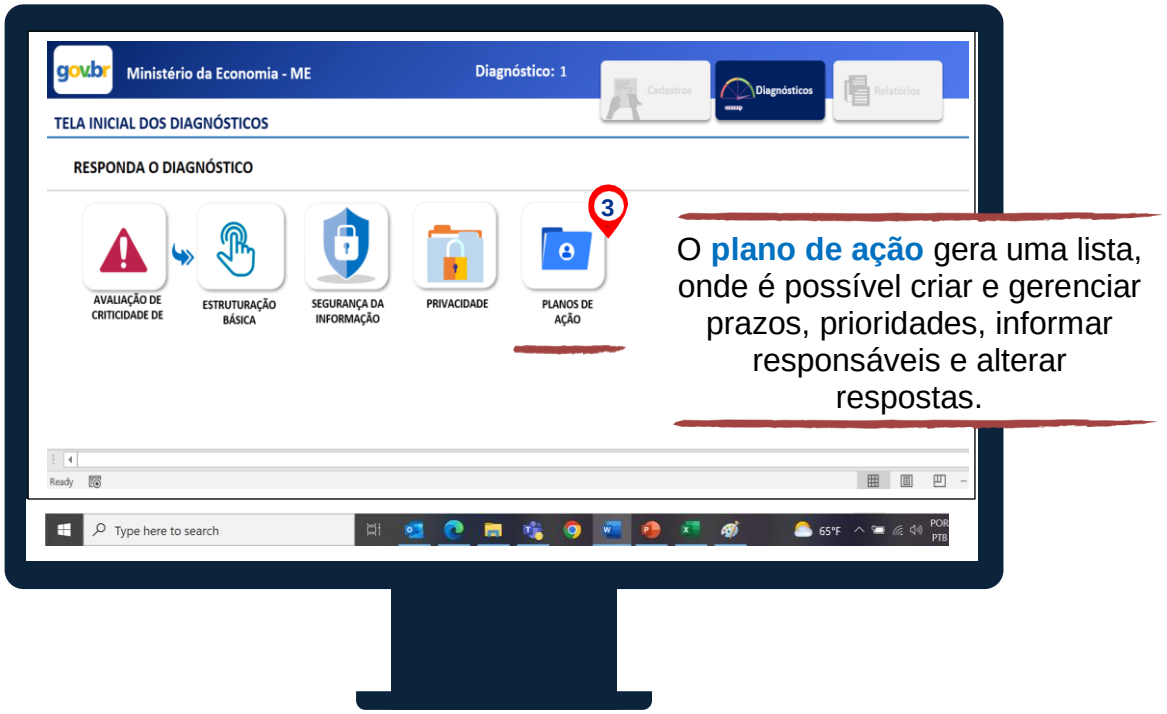
FIQUE ATENTO!

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 Ação

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

4.9 Planos de Ação



O **plano de ação** gera 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 ação é importante clicar no botão "**Atualizar Lista de todos os Planos de ação**", em seguida aguardar carregar todos os planos de ação aplicáveis, para então preencher os demais campos do formulário do plano de ação.*

FIQUE ATENTO!

PLANOS DE AÇÃO

Atualizar Lista de Todos os Planos de Ação

1º Se estiver iniciado o preenchimento dos campos referente as medidas que precisam de plano de ação e clicar no **botão pela 2ª vez irá apagar todas as informações já preenchidas.**

Atualizar Todas as Novas Respostas

2º Se os planos de ação estiverem preenchidos, clicar no botão **atualizar resposta alterará todo histórico anterior**, e caso a medida que teve uma nova resposta **ainda for aplicável para o plano de ação**, irá aparecer na coluna **resposta principal** de acordo **com o que foi atualizado no botão de nova resposta**.

AVISO!!!

*Ao **alterar uma nova resposta** basta clicar em "**Atualizar Todas as Novas respostas**" para que possa **refletir no formulário no questionário principal**, de acordo com o identificador da medida (ID) para plano de ação, então vai aparecer na coluna de resposta principal de acordo com o que foi atualizado no botão de nova resposta.*

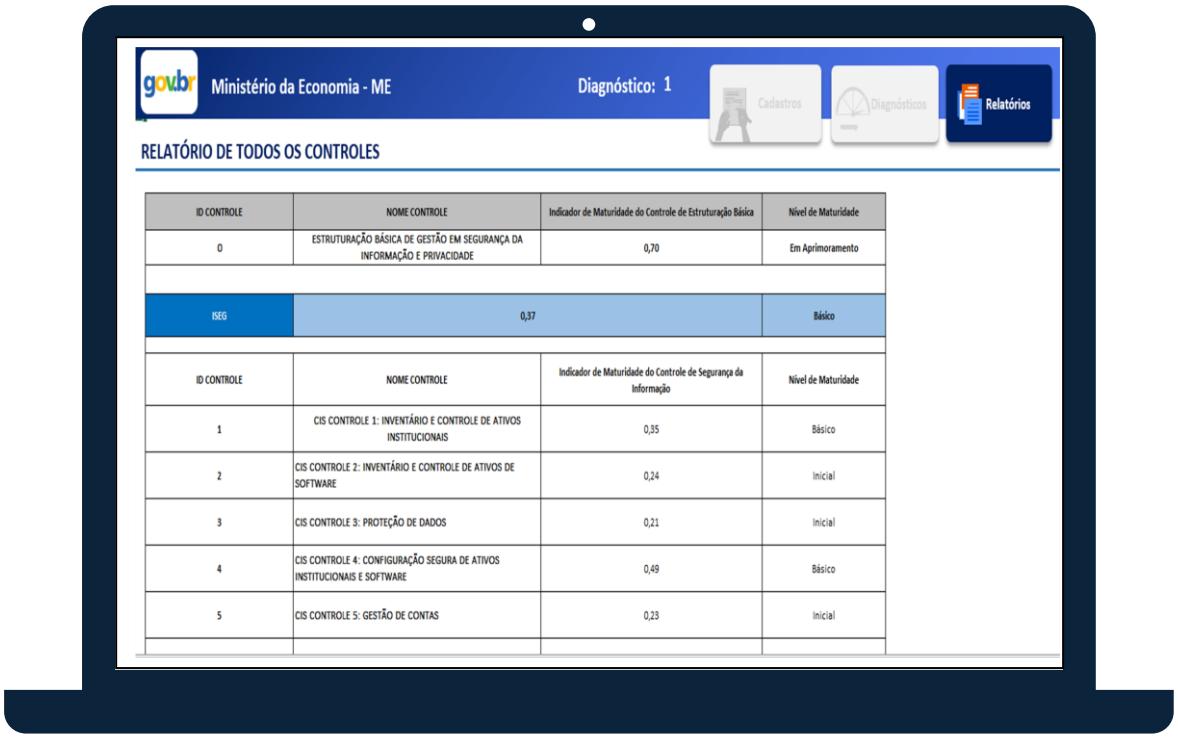
4.9.1 *Descrição de cada coluna:*

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 ação, 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 ação.	Esse campo é preenchido automaticamente, caso o usuário final tenha selecionado o responsável pelo plano de ação.
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 ação.	É **imprescindível** que preencha a data de previsão de início do plano de ação
9	**PREVISÃO DE FIM**	Serve para direcionar para o responsável a data fim do plano de ação.	É **imprescindível** que preencha a data de previsão de fim do plano de ação 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 ação (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 ação 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 ação 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.

5. RELATÓRIOS E DASHBOARDS

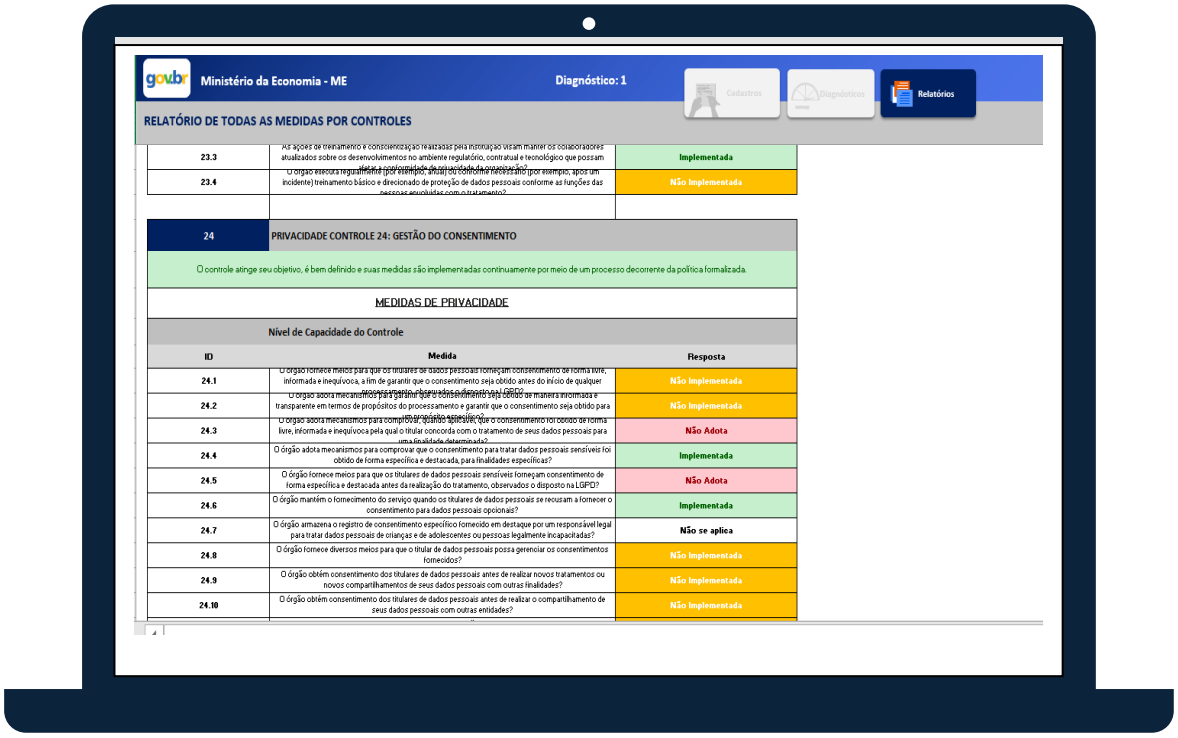
5.1 Relatórios



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	0,70	Em Aprimoramento
ISEG	0,37		Básico
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	0,35	Básico
2	CIS CONTROLE 2: INVENTÁRIO E CONTROLE DE ATIVOS DE SOFTWARE	0,24	Inicial
3	CIS CONTROLE 3: PROTEÇÃO DE DADOS	0,21	Inicial
4	CIS CONTROLE 4: CONFIGURAÇÃO SEGURA DE ATIVOS INSTITUCIONAIS E SOFTWARE	0,49	Básico
5	CIS CONTROLE 5: GESTÃO DE CONTAS	0,23	Inicial

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.



5.1.1 *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.

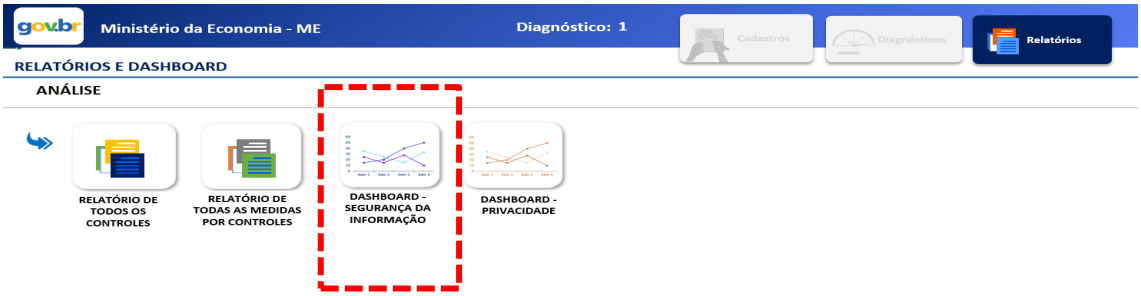
Não Implementada: O órgão não implementou a medida, ou seja, a medida foi respondida com algumas das opções abaixo:

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

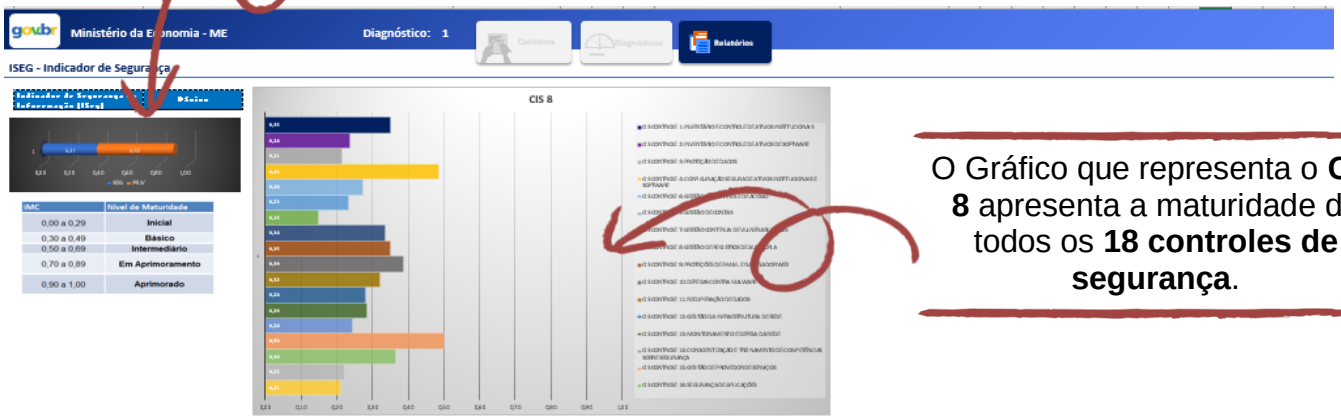
Implementada: O órgão implementou a medida, ou seja, a medida foi respondida com “Adota a medida integralmente em mais de 50% dos ativos”. Há decisão formal ou plano aprovado, e a medida é implementada integralmente na maioria (mais de 50%) ou em todos os ativos de informação da organização.

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.

5.2 Dashboard de Segurança da Informação



O Gráfico ISEG e IPRIV são os indicadores avaliados e calculados separadamente, gerando dois indicadores insolados.



O Gráfico que representa o **CIS 8** apresenta a maturidade de todos os **18 controles de segurança**.

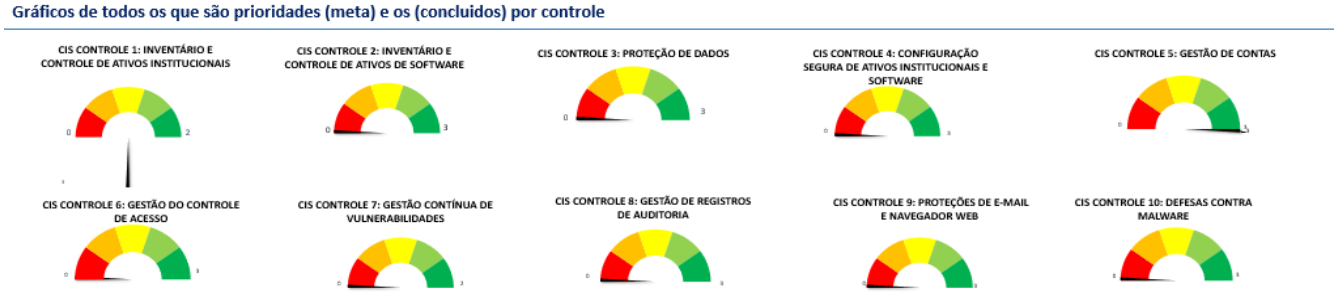
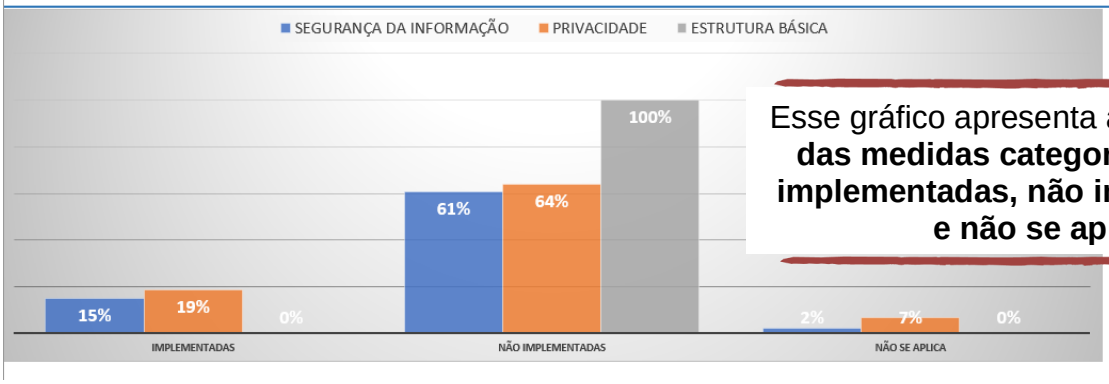


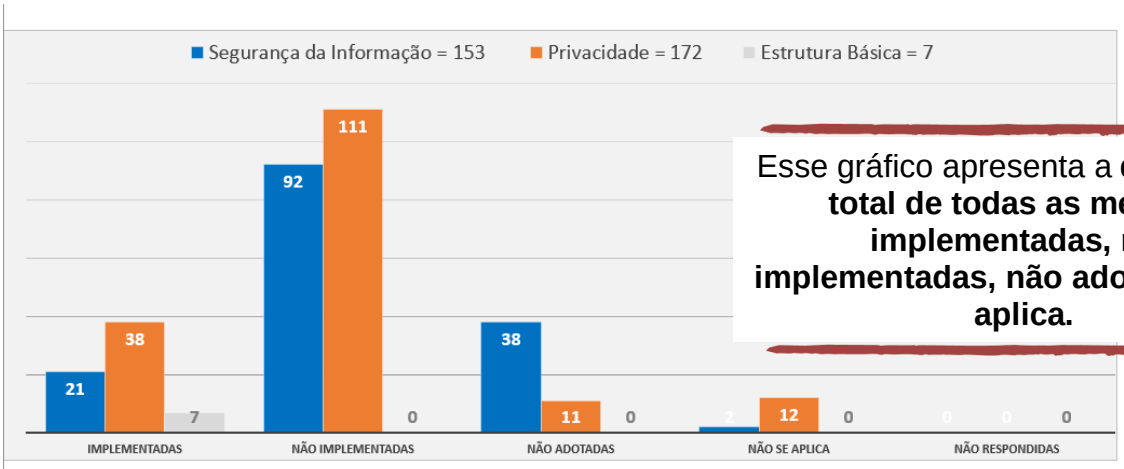
Gráfico com percentual implementado, não implementados e não se aplica



Esse gráfico apresenta a **porcentagem das medidas categorizadas como implementadas, não implementadas e não se aplica**.

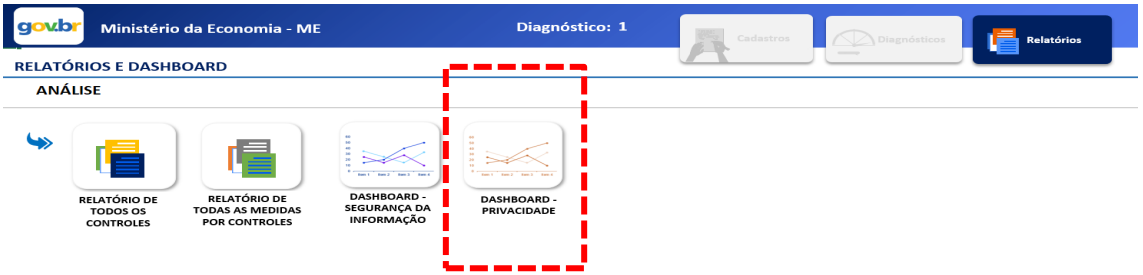
AVISO!!!

*Os **gráficos** apresentam a **quantidade** de **medidas** que foram **priorizadas**, além de mostrar a evolução de sua implementação.*

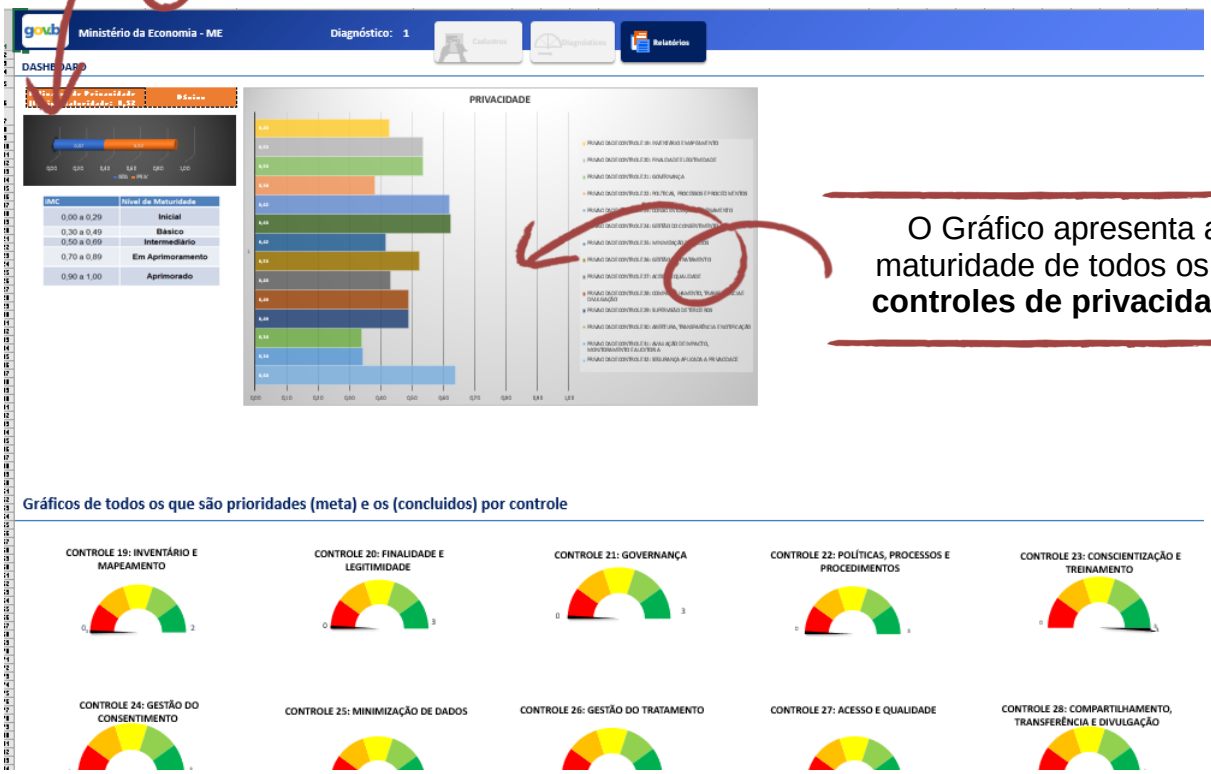


Esse gráfico apresenta a **quantidade total de todas as medidas implementadas, não implementadas, não adota e não se aplica.**

5.3 Dashboard de Privacidade



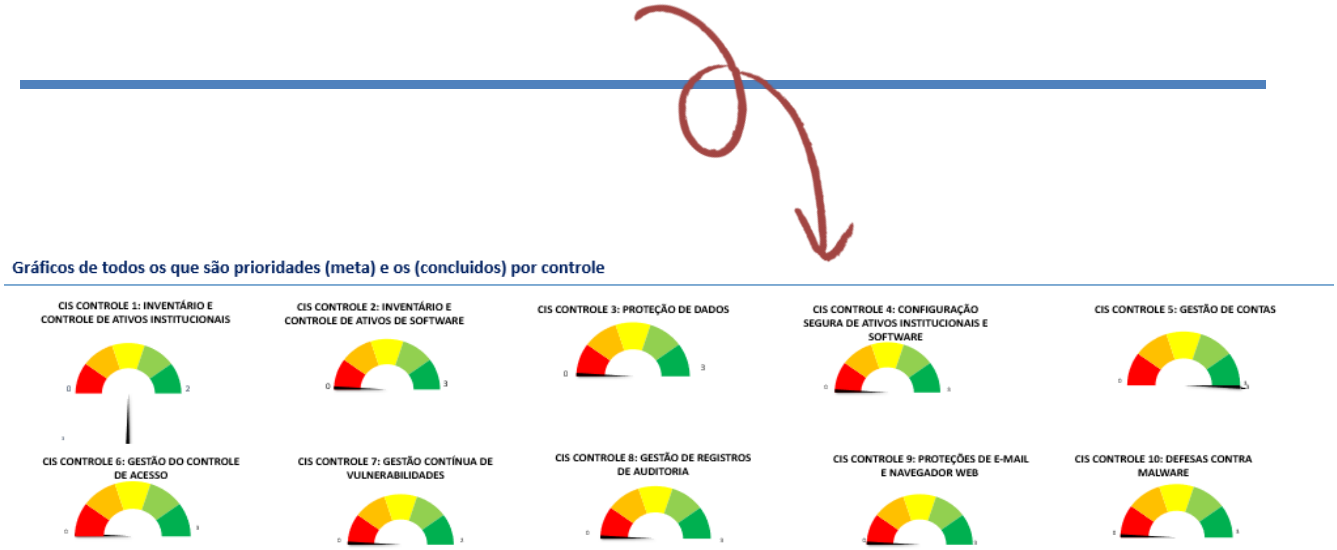
O Gráfico ISEG e IPRIV são os indicadores avaliados e calculados separadamente, gerando dois indicadores insolados.



O Gráfico apresenta a maturidade de todos os **13 controles de privacidade**.

5.4 Gráficos de Controles por Prioridade (Segurança da Informação e Privacidade)

Os Gráficos de prioridades informam as quantidades de medidas priorizadas em cada controle e contabiliza quantas foram concluídas. Você encontra esse gráfico no Dashboard de Segurança da Informação e no de Privacidade.

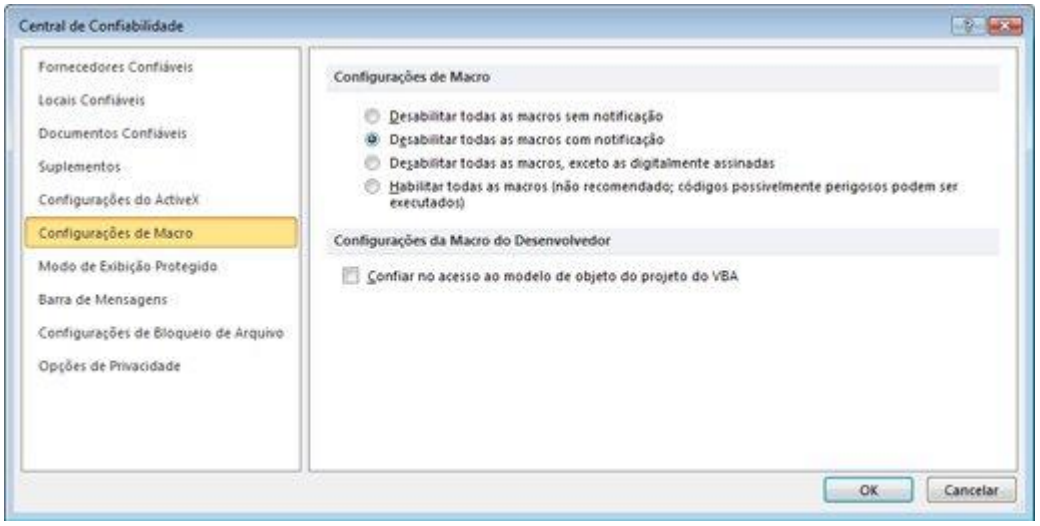


ANEXO I – HABILITAR MACROS EM ARQUIVOS DO OFFICE 365

As configurações de macro estão localizadas na Central de Confiabilidade. Importante ressaltar que se, o dispositivo for gerenciado pelo seu trabalho, o administrador do sistema poderá impedir que qualquer pessoa tenha acesso ou altere as configurações, por isso a necessidade de consultar o setor de Tecnologia da Informação antes.

Para HABILITAR a macro siga os passos abaixo que também podem ser consultados no site do fabricante[5]:

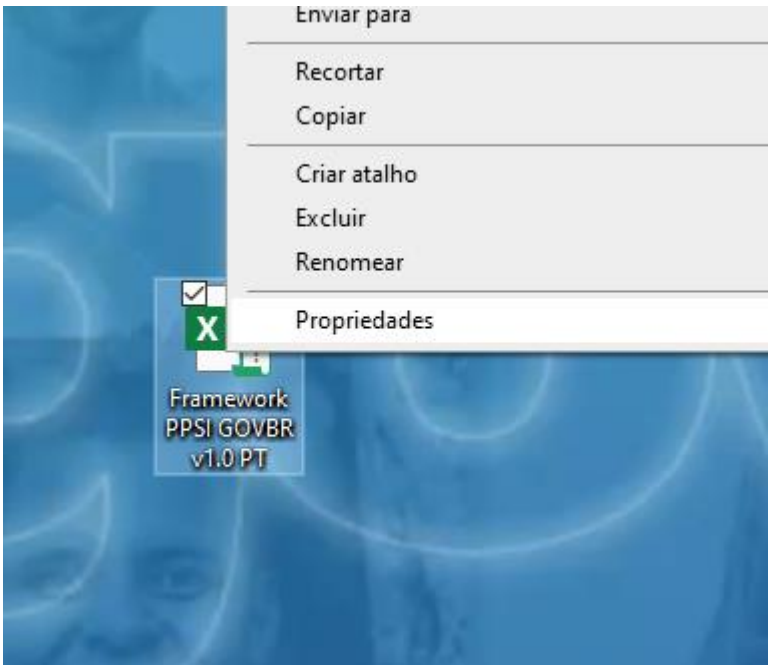
1. Clique na guia **Arquivo**.
2. Clique em **Opções**.
3. Clique em **Central de Confiabilidade** e em **Configurações da Central de Confiabilidade**.
4. Na **Central de Confiabilidade**, clique em **Configurações de Macro**.



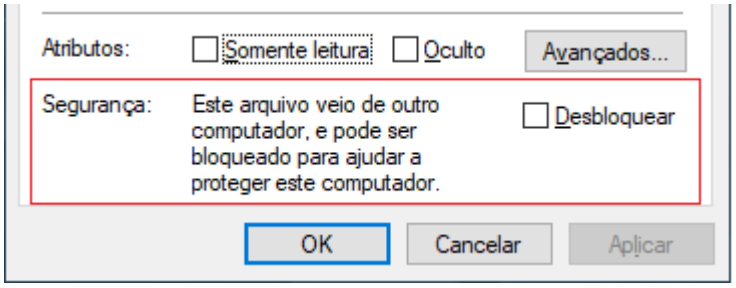
5. Faça as seleções desejadas e clique em **OK**.

[5] Disponível em: https://support.microsoft.com/pt-br/office/habilitar-ou-desabilitar-macros-em-arquivos-do-office-12b036fd-d140-4e74-b45e-16fed1a7e5c6

Além de habilitar a macro, pode ser necessário também o DESBLOQUEIO do arquivo, que pode ser feito acessando suas PROPRIEDADES:



Na janela de PROPRIEDADES marque a opção “DESBLOQUEAR”.



Pronto, seu arquivo estará liberado para uso em sua máquina.

Dúvida? Entre em contato conosco.

Email: cgpd@economia.gov.br

Telefone: (61) 2020-2046

DEPARTAMENTO DE
PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

SECRETARIA DE
GOVERNO DIGITAL

MINISTÉRIO DA
ECONOMIA