

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	6
1. INTRODUÇÃO	7
2. FERRAMENTA E ESTRUTURAÇÃO BÁSICA DE GESTÃO	8
3. CADASTRO DO ÓRGÃO	9
3.1 ADICIONAR O NOME DO ÓRGÃO	9
3.2 ADICIONAR CONTATOS DOS RESPONDENTES	10
3.3 ADICIONAR CADASTRO DO RESPONSÁVEL/DEPARTAMENTO DOS PLANOS DE AÇÃO	11
3.4 NOTA TÉCNICA	12
4. DIAGNÓSTICO	13
4.1 AVALIAÇÃO DE CRITICIDADE DE SISTEMAS	13
4.2 DIAGNÓSTICOS DE ESTRUTURAÇÃO BÁSICA, DIAGNÓSTICO DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE.	15
4.3 ESTRUTURAÇÃO BÁSICA DE GESTÃO EM PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO	16
4.4 DIAGNÓSTICO DE SEGURANÇA DA INFORMAÇÃO	17
4.5 DIAGNÓSTICO DE PRIVACIDADE	18
4.6 LEGENDA DA LISTA DE OPÇÃO DE RESPOSTA	19
4.7 LISTA DE RESPOSTAS DOS DIAGNÓSTICOS DE SI E PRIVACIDADE	19
4.8 LISTA DE RESPOSTAS QUALITATIVA	20
4.9 PLANOS DE AÇÃO	22
4.9.1 Descrição de cada coluna:	24
5. RELATÓRIOS E DASHBOARDS	26
5.1 RELATÓRIOS	26
5.1.1 Quais são as opções de implementação?	27
5.2 DASHBOARD DE SEGURANÇA DA INFORMAÇÃO	28
5.3 DASHBOARD DE PRIVACIDADE	30
5.4 GRÁFICOS DE CONTROLES POR PRIORIDADE (SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE)	31
ANEXO I – HABILITAR MACROS EM ARQUIVOS DO OFFICE 365	33

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 operacionais³ 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 informação⁴.

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**.

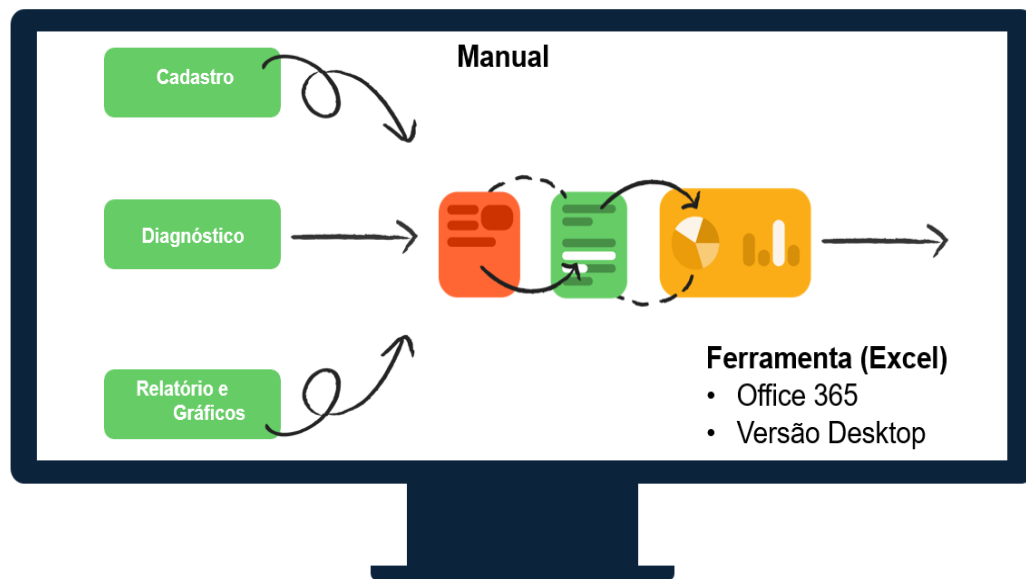
Cabe ressaltar que ao utilizar a **Ferramenta do Framework de Privacidade e Segurança da Informação** é imprescindível a utilização da versão aplicável ao idioma do pacote office 365 instalado na máquina onde será utilizado.

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>

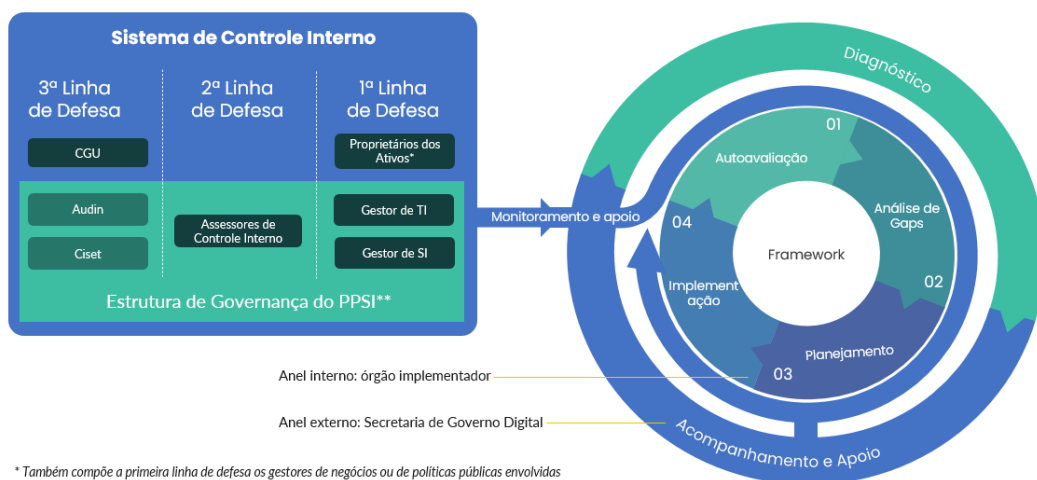
³ Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias-operacionais-para-adequacao-a-lei-geral-de-protecao-de-dados-pessoais-lgpd>

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.



* 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 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

gouvernamento.br Ministério da Economia - ME Diagnóstico: 1

PRIMEIROS PASSOS

Por favor, informe seu órgão: **Ministério da Economia - ME**

Nome do Responsável 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

OUTROS		NOTA TÉCNICA	
Nome do Órgão:	*	Nº do Documento	2022/0509
CNPJ:	*	Qual é o Diagnóstico?	1
		Data Fim do envio do Diagnóstico:	05/09/2022



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 Responsável 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

The screenshot shows a web application interface with a form for adding responsible parties and departments for action plans. The form is divided into two main sections: 'PRIMEIROS PASSOS' (First Steps) and 'PLANOS DE AÇÃO' (Action Plans). The 'PRIMEIROS PASSOS' section includes fields for Name, CNPJ, and Email. The 'PLANOS DE AÇÃO' section includes a table for adding responsible parties and departments. A red arrow points from the 'PRIMEIROS PASSOS' section to the text below.

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

gondx Diagnóstico: Cadastros Diagnósticos Relatórios

PRIMEIROS PASSOS

Por favor, informe seu órgão:

Nome do Responsável pela Unidade de Controle Interno:	Nome_Responsável_ControleInterno	Nome do Gestor de Segurança da Informação:	Nome_Responsável_SI
E-mail do Respondente:	Nome_Responsável@orgao.com	E-mail do Respondente:	Nome_Responsável@orgao.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@orgao.com	E-mail do Respondente:	Nome_Responsável@orgao.com

OUTROS

Nome do Órgão:	*
CNPJ:	*

USO DA SGD

Nº do Documento (Nota Técnica):	
Versão do Diagnóstico enviado:	
Data Limite para retorno do Diagnóstico:	

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

DADOS DO RETORNO DO DIAGNÓSTICO PARA SGD

Data de retorno do Diagnóstico para SGD:	
Versão do Diagnóstico devolvido:	

Nota Técnica

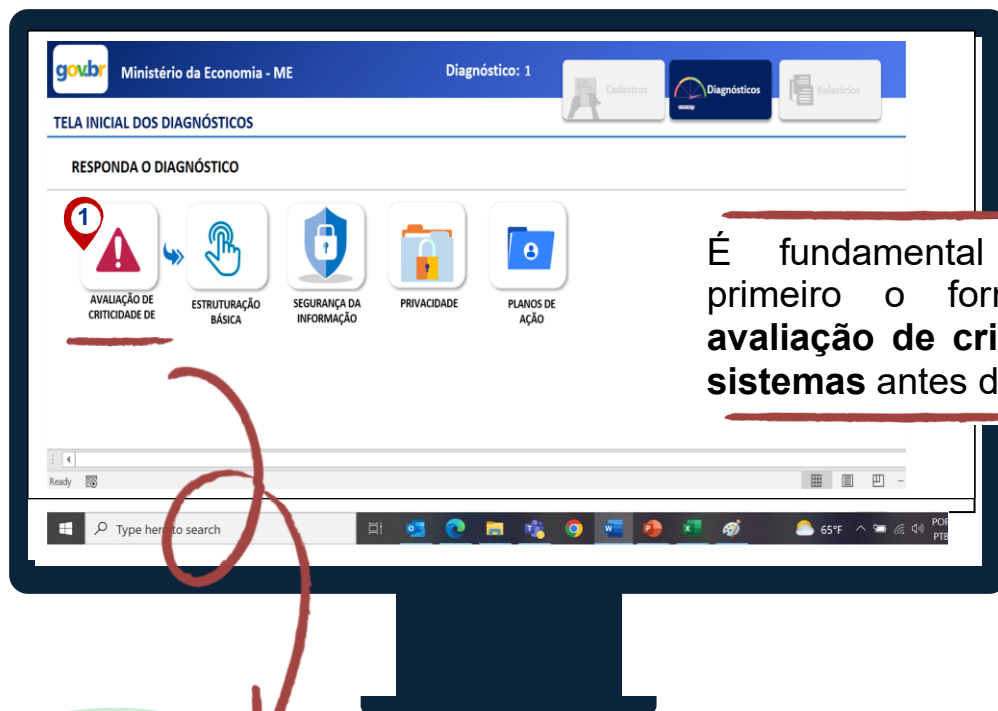
Todos os campos (número do documento, diagnóstico e a data final de envio) serão preenchidos pela SGD de acordo com a nota técnica.

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>



gov.br Ministério da Economia - ME Diagnóstico: 1

AVALIAÇÃO DE CRITICIDADE DE SISTEMAS

A Instituição já utiliza uma metodologia de para avaliação de criticidade de ambiente tecnológico do seus sistemas?

Se a resposta for SIM: Por favor, selecione a opção correta no campo em amarelo, considerando o Sistema de Nivel de Criticidade mais ALTO.

Se a Resposta for NÃO: 1º Passo: Por favor, responder ao Questionário de Avaliação e Criticidade; 2º Passo: Após obter a Informação do Nivel de criticidade, selecione a opção correta no campo em amarelo, considerando o Sistema de Nivel de Criticidade mais ALTO.

Nivel de Criticidade Grupo de Implementação

Baixa Criticidade G2

Clicar Apenas 1x - Após Saber o Grupo de Implementação

Esse formulário é o primeiro a ser preenchido.

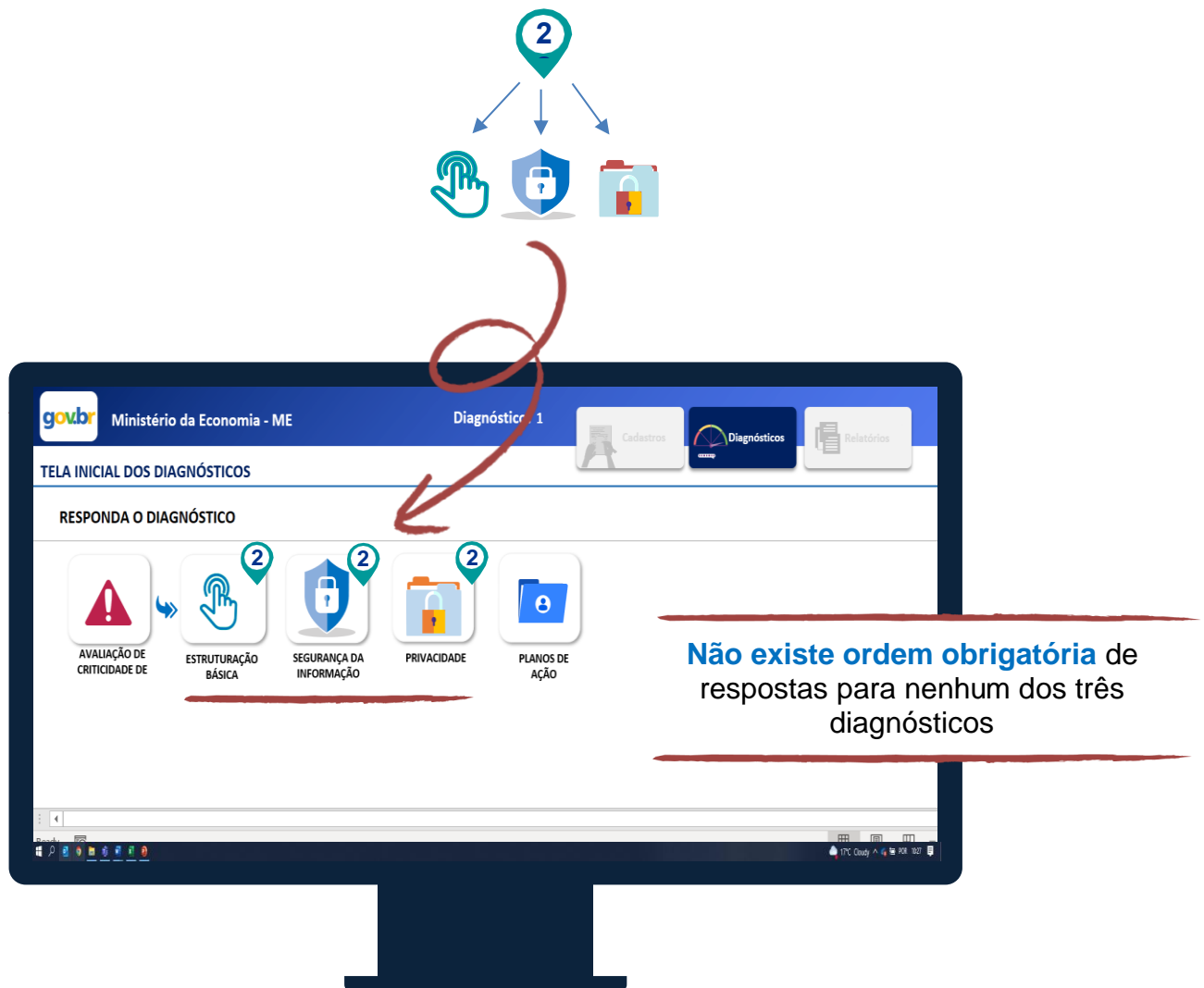
Selecione a resposta e siga as orientações de acordo com o que foi respondido (caixa VERDE ou VERMELHA). O nível de criticidade deve ser selecionado de acordo com a criticidade do sistema relevante mais crítico selecionado pelo órgão, essa informação definirá o Grupo de implementação em que o órgão se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



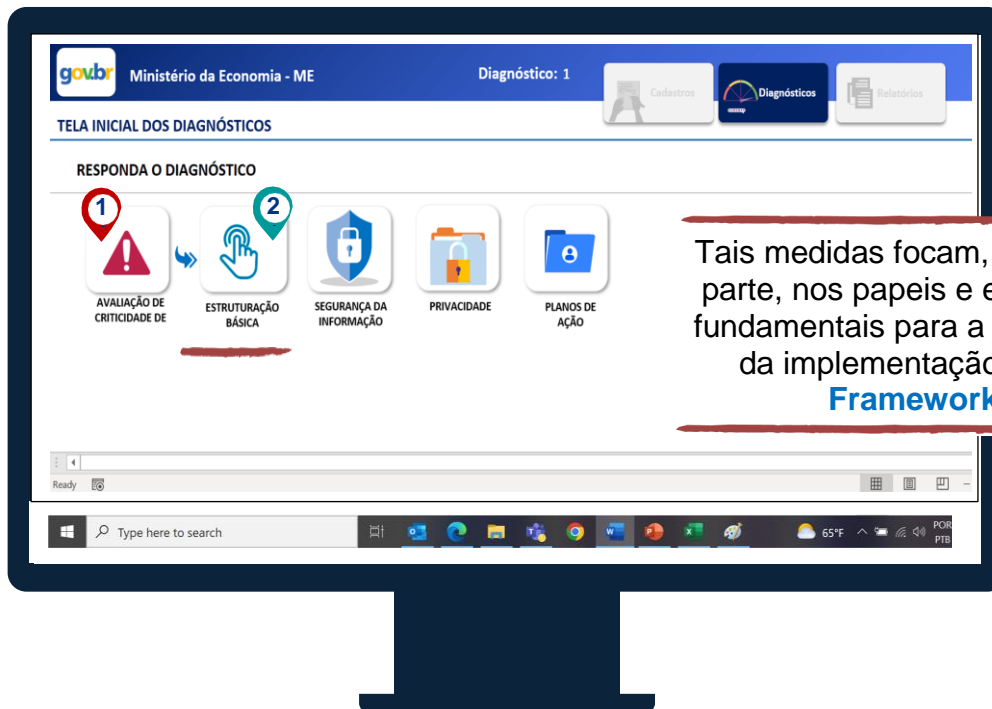
4.2 Diagnósticos de Estruturação básica, Diagnóstico de Segurança da Informação e Privacidade.



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.

**Estruturação
Básica**

4.3 Estruturação básica de gestão em privacidade e segurança da informação



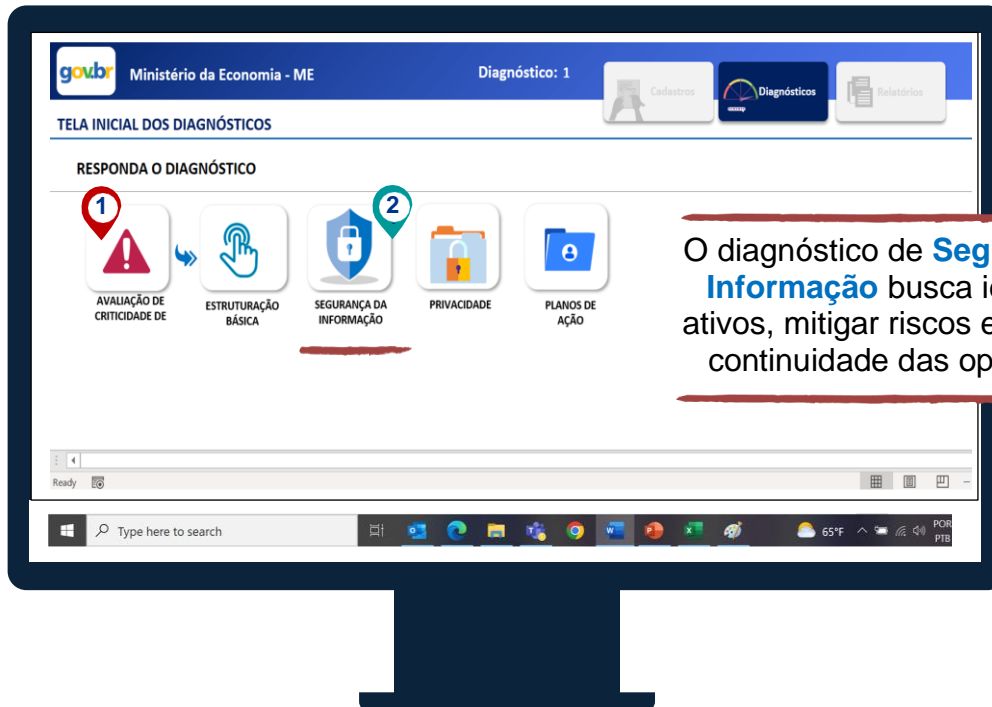
Tais medidas focam, em maior parte, nos papéis e estruturas fundamentais para a condução da implementação deste **Framework**

ID	MEDIDA	DESCRIÇÃO	RESPOSTA
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.	Sim
0.2	O órgão nomeou um Gestor de Segurança da	O Gestor de Segurança da Informação é responsável primário por planejar, implementar e melhorar continuamente os controles de segurança da	Sim



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.

gov.br Ministério da Economia - ME Diagnóstico: 1

SEGURANÇA DA INFORMAÇÃO

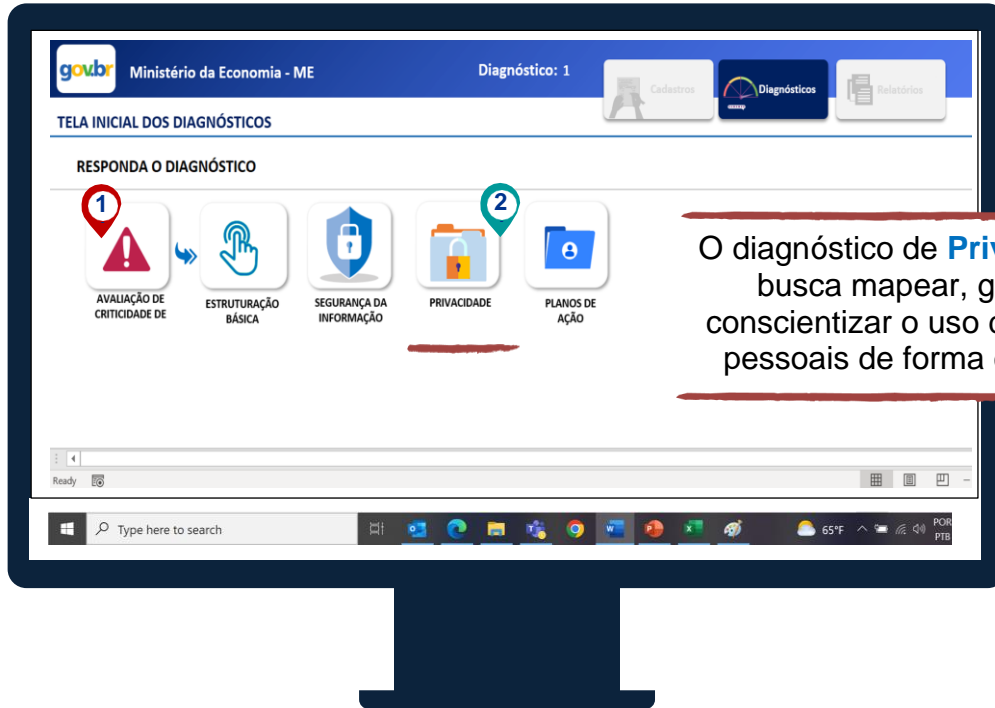
Aviso O formulário de Avaliação de Criticidade de Sistemas foi preenchido corretamente. Lembrou de clicar no botão para atualizar as opções de respostas desse diagnóstico de segurança da informação?

Controles CIS Versão 8									
FILTRO	ID	ID CIS	GRUPO IMPL	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	RESPOSTAS	Questionário Qualitativo	
1 CIS CONTROLE 1: INVENTÁRIO E CONTROLE DE ATIVOS INSTITUCIONAIS									
1	1.1	1.1	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 eletrônico), endereço de hardware, nome da máquina, etc. Deverá incluir ativos conectados à infraestrutura física, virtual, e remota e aqueles dentro de ambiente de nuvem. Necessário incluir também ativos móveis que não estejam sob controle do órgão. Revisar e atualizar o inventário semestralmente ou com mais frequência.	Adota parcialmente	O controle atinge seu objetivo por meio da aplicação de um conjunto básico, porém completo, de atividades que podem ser caracterizadas como realizadas.	



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.

Ministério da Economia - ME						
PRIVACIDADE				Diagnóstico: 1		
ID	GRUPO DE IMPLEMENTAÇÃO	FUNÇÃO NIST PF	MEDIDA	RESPOSTA	Justificativa do porquê da resposta "Não se aplica"	NÍVEL DE CAPACIDADE DE TODO O CONTROLE
19	CONTROLE 19: INVENTÁRIO E MAPEAMENTO					2
19.1	G1	IDENTIFICAR-P	A organização documenta os sistemas, serviços e processos que tratam dados pessoais?	Adota em menor parte		<input type="checkbox"/> controle atinge seu objetivo por meio da aplicação de um conjunto básico, porém completo, de atividades que podem ser caracterizadas como realizadas.



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

4.6 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						CIS CONTROLE 5: GESTÃO DE CONTAS			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	Selecione a Resposta		

4.7 Lista de Respostas dos Diagnósticos de SI e Privacidade

RESPOSTAS

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 medida
- 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: <ul style="list-style-type: none"> - 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: <ul style="list-style-type: none"> - 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: <ul style="list-style-type: none"> - 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: <ul style="list-style-type: none"> - 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



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 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!

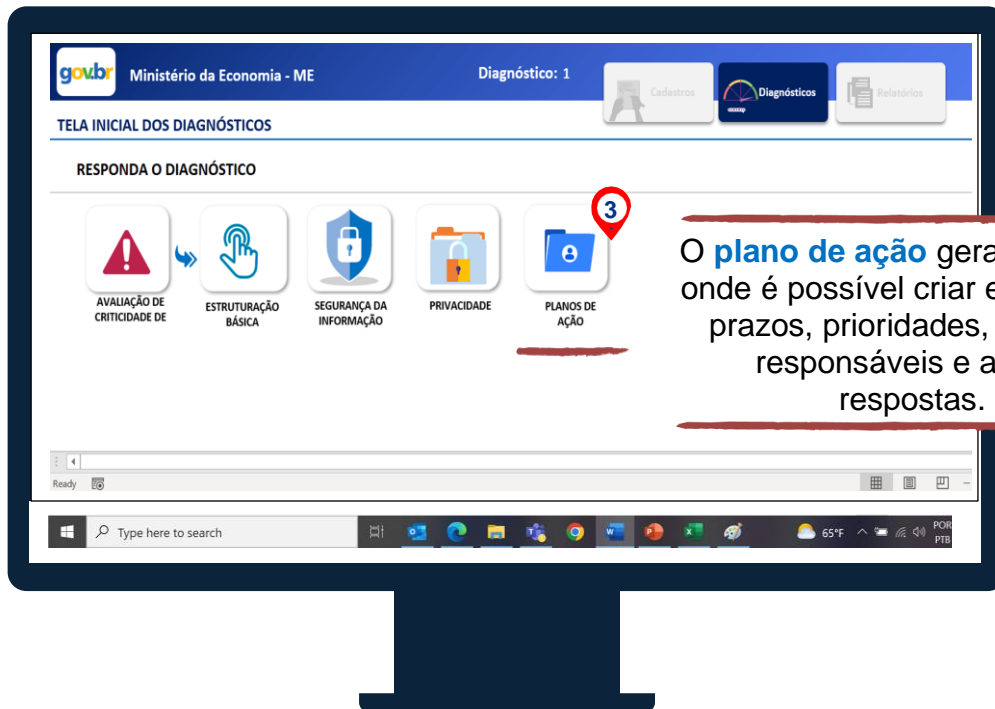
As respostas influenciam no cálculo da maturidade, ou seja, é importante avaliar em qual das opções de descrição melhor responde a medida do formulário.



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



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.

Ministério da Economia - ME | Diagnóstico: 1

PLANOS DE AÇÃO

Atualizar Lista de Todos os Planos de Ação | Atualizar Todas as Novas Respostas

QTD TOTAL DE PLANOS DE AÇÃO: 259 | QTD PLANOS DE AÇÃO COM PRIORIDADE: 43

ID	MEDIDA	RESPOSTA	Encaminhamento interno (o órgão faz o preenchimento manual)	Responsável	Departamento	Observação do Órgão p
0.3	O órgão nomeou um responsável pela unidade de controle interno?	Não	FRAMEWORK	SURICATO-01	SALA-01	SGD-OSERVAÇÃO
0.4	O órgão instituiu um Comitê de Segurança da Informação?	Não	FRAMEWORK	SURICATO-02	SALA-02	SGD-OSERVAÇÃO

Resposta principal

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:

Ministério da Economia - ME													
Diagnóstico: 1													
S DE AÇÃO													
Atualizar Lista de Todos os Planos de Ação													
Atualizar Todas as Novas Respostas													
1	259	2	43	4	6	8	10	12					
QTD TOTAL DE PLANOS DE AÇÃO	QTD PLANOS DE AÇÃO COM PRIORIDADE	Encaminhamento interno (o órgão faz o preenchimento manual)	Responsáveis	Departamento	Observação do Órgão p SGO	Previsão de Início	Previsão de Fim	Status PA	Status Medida	Novas respostas	Prioridade		
0.3	O órgão nomeou um responsável pela unidade de controle interno?	Não	FRAMEWORK	SALA-01	SGO-OS	04/09/2022	10/09/2022	Atrasado	Não Finalizado	Sim	Não	13	
0.4	O órgão instituiu um Comitê de Segurança da Informação?	Não	FRAMEWORK	SURICATO-02	SALA-02	SGO-OBSERVAÇÃO	05/09/2022	10/09/2022	Atrasado	Não	Não		
0.5	O órgão instituiu uma Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETR?	Não	FRAMEWORK	SURICATO-03	SALA-03	SGO-OBSERVAÇÃO	06/09/2022	10/09/2022	Concluído	Finalizado	Não	Sim	
0.6	O órgão elaborou uma Política de Segurança da Informação - POSI?	Não	FRAMEWORK	SURICATO-04	SALA-04	SGO-OBSERVAÇÃO	07/09/2022	10/09/2022	Concluído	Finalizado	Não	Sim	
0.7	O órgão nomeou um Encarregado pelo	Não	FRAMEWORK	SALA-05	SGO-OBSERVAÇÃO	08/09/2022	10/09/2022	Atrasado	Não Finalizado	Sim	Não		

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 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 significativa.
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


Ministério da Economia - ME

Diagnóstico: 1


Cadastros


Diagnósticos


Relatórios

RELATÓRIOS E DASHBOARD


ANÁLISE


RELATÓRIO DE TODOS OS CONTROLES



RELATÓRIO DE TODAS AS MEDIDAS POR CONTROLES



DASHBOARD - SEGURANÇA DA INFORMAÇÃO



DASHBOARD - PRIVACIDADE


Ministério da Economia - ME

Diagnóstico: 1


Cadastros


Diagnósticos



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	0,70	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.



Ministério da Economia - ME

Diagnóstico: 1

Calendário

Relatório

RELATÓRIO DE TODAS AS MEDIDAS POR CONTROLES

23.3	As ações de treinamento e conscientização realizadas pela organização visam manter os colaboradores atualizados sobre os desenvolvimentos no ambiente regulatório, contratual e tecnológico que possam afetar a implementação das medidas de proteção de dados pessoais?	Implementada
23.4	O órgão elabora regulamento interno, atualiza os procedimentos internos por exemplo, tipos de incidentes (tratamento básico e direcionado de proteção de dados pessoais) conforme as mudanças das normas aplicáveis com o tratamento?	Não Implementada
24	PRIVACIDADE CONTROLE 24: GESTÃO DO CONSENTIMENTO	
O controle atinge seu objetivo, é bem definido e suas medidas são implementadas continuamente por meio de um processo decorrente da política formalizada.		
MEDIDAS DE PRIVACIDADE		
Nível de Capacidade do Controle		
ID	Medida	Resposta
24.1	O órgão fornece meios para que os titulares de dados possam dar consentimento de forma livre, informada e inequívoca, a fim de garantir que o consentimento seja obtido antes do início de qualquer tratamento de dados pessoais?	Não Implementada
24.2	O órgão adota mecanismos para garantir que o consentimento seja obtido de maneira transparente em termos de propósitos do processamento e garantir que o consentimento seja obtido para cada finalidade de tratamento?	Não Implementada
24.3	O órgão adota mecanismos para comprovar que o consentimento foi obtido de forma livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada?	Não Adota
24.4	O órgão adota mecanismos para comprovar que o consentimento para tratar dados pessoais sensíveis foi obtido de forma específica e destacada, para a finalidade específica?	Implementada
24.5	O órgão fornece meios para que os titulares de dados pessoais possam dar consentimento de forma específica e destacada antes da realização do tratamento, observados o disposto na LGPD?	Não Adota
24.6	O órgão mantém o fornecimento do serviço quando os titulares de dados pessoais se recusam a fornecer o consentimento para a dados pessoais opcionais?	Implementada
24.7	O órgão mantém o registro de consentimento específico fornecido em destaque por um responsável legal para tratar dados pessoais de crianças e de adolescentes ou pessoas legalmente incapazes?	Não se aplica
24.8	O órgão fornece diversos meios para que o titular de dados pessoais possa gerenciar os consentimentos fornecidos?	Não Implementada
24.9	O órgão obtém consentimento dos titulares de dados pessoais antes de realizar novos tratamentos ou novos compartilhamentos de seus dados pessoais com outras finalidades?	Não Implementada
24.10	O órgão obtém consentimento dos titulares de dados pessoais antes de realizar o compartilhamento de seus dados pessoais com outras entidades?	Não Implementada

2

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

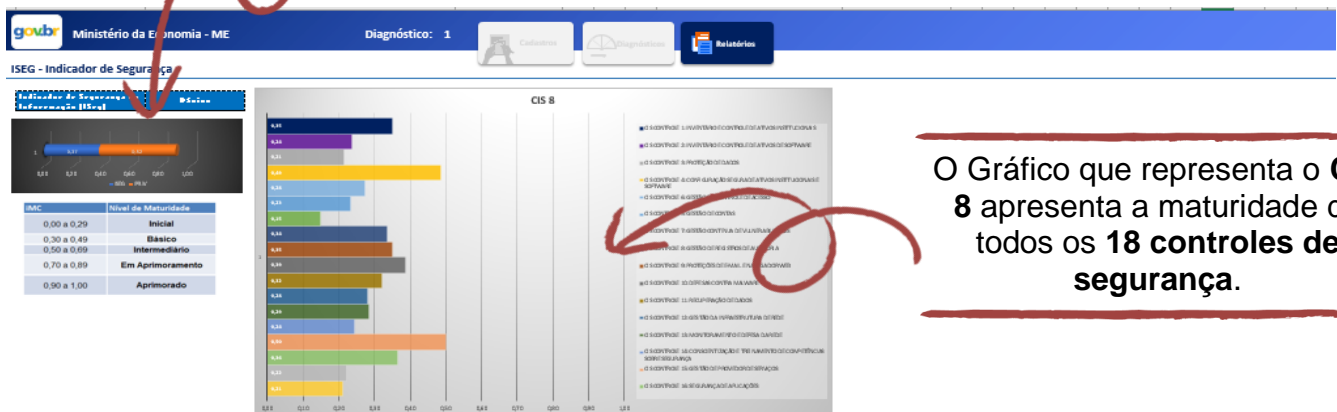
Implementada: O órgão implementou a medida, ou seja, a medida foi respondida com “Adota a medida integralmente em mais de 50% dos ativos”. Há decisão formal ou plano aprovado, e a medida é implementada integralmente na maioria (mais de 50%) ou em todos os ativos de informação da organização.

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.

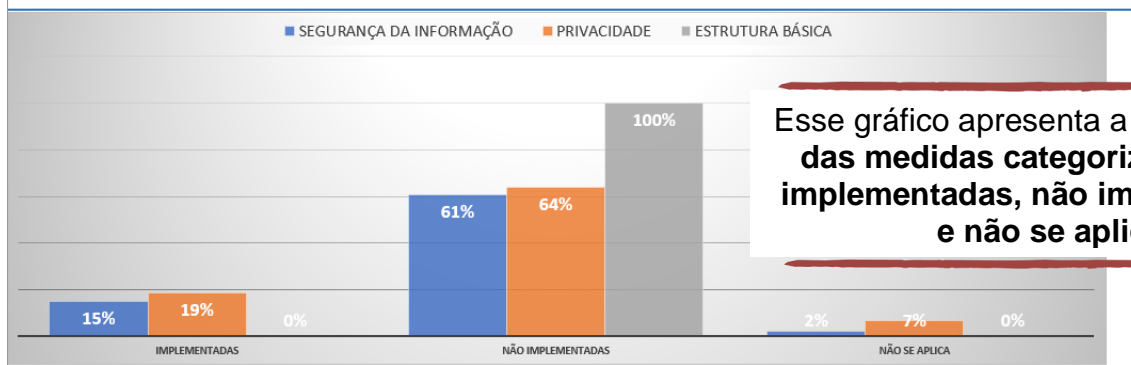


O Gráfico que representa o **CIS 8** apresenta a maturidade de todos os **18 controles de segurança**.

Gráficos de todos os que são prioridades (meta) e os (concluídos) por controle

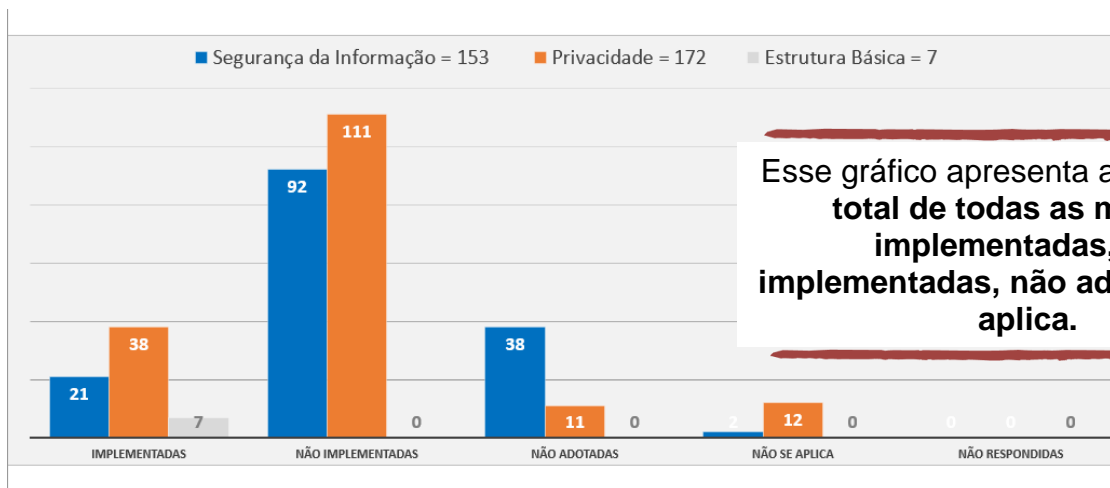


Gráfico com percentual implementado, não implementados e não se aplica



AVISO!!!

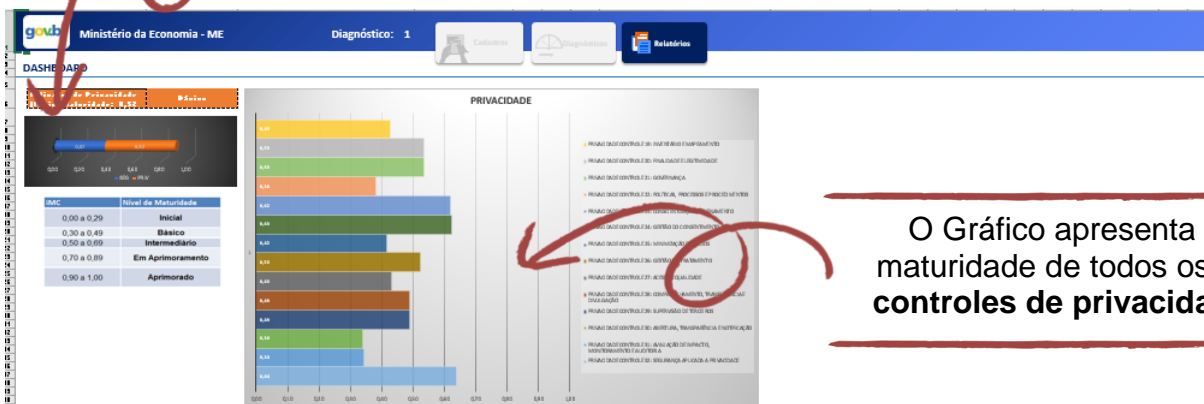
Os **gráficos** apresentam a **quantidade** de **medidas** que foram **priorizadas**, além de mostrar a **evolução** de sua **implementação**.



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.

Gráficos de todos os que são prioridades (meta) e os (concluídos) por controle

CONTROLE 19: INVENTÁRIO E MAPEAMENTO



CONTROLE 20: FINALIDADE E LEGITIMIDADE



CONTROLE 21: GOVERNANÇA



CONTROLE 22: POLÍTICAS, PROCESSOS E PROCEDIMENTOS



CONTROLE 23: CONSCIENTIZAÇÃO E TREINAMENTO



CONTROLE 24: GESTÃO DO CONSENTIMENTO



CONTROLE 25: MINIMIZAÇÃO DE DADOS



CONTROLE 26: GESTÃO DO TRATAMENTO



CONTROLE 27: ACESSO E QUALIDADE



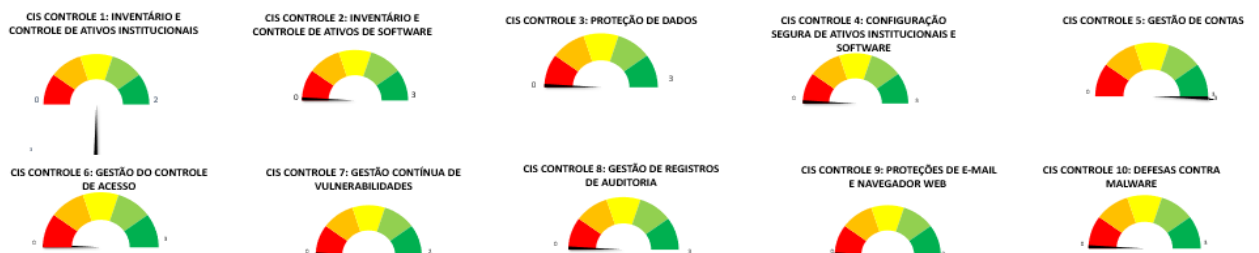
CONTROLE 28: COMPARTILHAMENTO, TRANSFERÊNCIA E DIVULGAÇÃO



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

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

Gráficos de todos os que são prioridades (meta) e os (concluídos) por controle

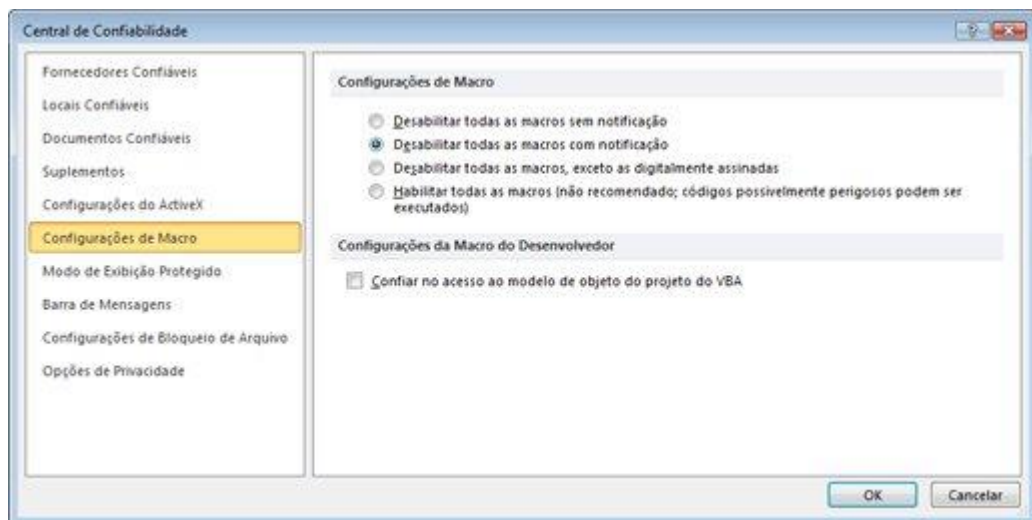


ANEXO I – HABILITAR MACROS EM ARQUIVOS DO OFFICE 365

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 fabricante⁵:

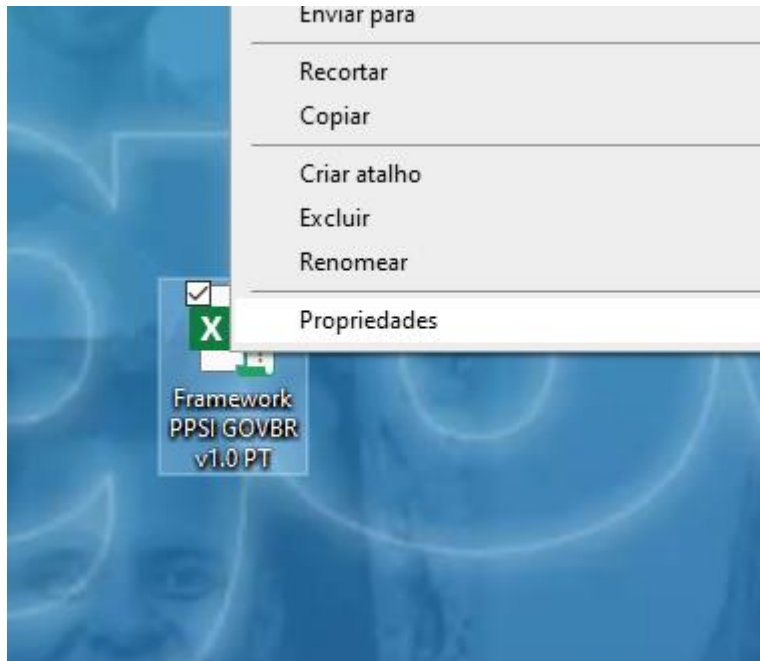
1. Clique na guia **Arquivo**.
2. Clique em **Opções**.
3. Clique em **Central de Confiabilidade** e em **Configurações da Central de Confiabilidade**.
4. Na **Central de Confiabilidade**, clique em **Configurações de Macro**.



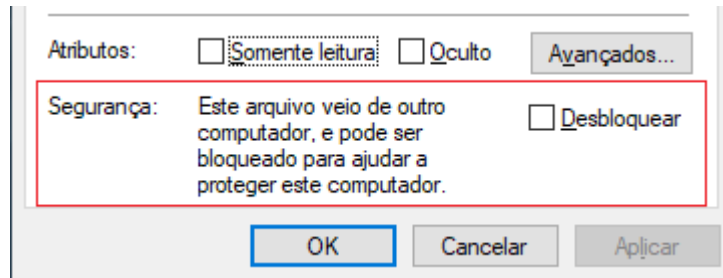
5. Faça as seleções desejadas e clique em **OK**.

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