# Plano de Proteção de Dados da Presidência da República

1ª edição
Brasília/DF, 2022

PRESIDÊNCIA DA REPÚBLICA

COMITÊ DE GOVERNANÇA DIGITAL E SEGURANÇA DA INFORMAÇÃO DA PRESIDÊNCIA DA REPÚBLICA

COMISSÃO DE PROTEÇÃO DE DADOS DA PRESIDÊNCIA DA REPÚBLICA

# PLANO DE PROTEÇÃO DE DADOS DA PRESIDÊNCIA DA REPÚBLICA

Brasília – DF

Março de 2022

JAIR MESSIAS BOLSONARO
Presidente da República

ANTONIO HAMILTON MARTINS MOURÃO
Vice-Presidente da República

CIRO NOGUEIRA
Ministro de Estado Chefe da Casa Civil

FLÁVIA ARRUDA
Ministra de Estado Chefe da Secretaria de Governo

LUIZ EDUARDO RAMOS
Ministro de Estado Chefe da Secretaria-Geral

AUGUSTO HELENO RIBEIRO PEREIRA
Ministro de Estado Chefe do Gabinete de Segurança Institucional

CÉLIO FARIA JÚNIOR
Chefe do Gabinete Pessoal do Presidente da República

JOÃO HENRIQUE NASCIMENTO DE FREITAS
Assessor-Chefe da Assessoria Especial do Presidente da República

FLÁVIO AUGUSTO VIANA ROCHA
Secretário Especial de Assuntos Estratégicos

# FICHA TÉCNICA

**Comitê de Governança Digital e Segurança da Informação da Presidência da República**

Mario Fernandes (Titular); Vanessa Ferreira de Lima (Suplente) - Secretaria-Geral (Coordenação)

Célio Faria Junior (Titular); Carlos Henrique C. de Oliveira (Suplente) - Gabinete Pessoal do Presidente da República

João Henrique N. de Freitas (Titular) - Assessoria Especial do Presidente da República

Jonathas Assunção Salvador Nery de Castro (Titular); Juliana Ribeiro Silveira (Suplente) - Casa Civil

Carlos Henrique Menezes Sobral (Titular); Viviane de Faria (Suplente) - Secretaria de Governo

Carlos José R. A. Penteado (Titular); Osmar L. Machado (Suplente) - Gabinete de Segurança Institucional

Flávio Augusto V. Rocha (Titular); Joanisval B. Gonçalves (Suplente) - Secretaria Especial de Assuntos Estratégicos

Cesar Leme Justo (Titular); Álvaro Goncalves Wanderley (Suplente) - Vice-Presidência da República

Antonio Carlos Paiva Futuro (Titular); Clóvis Curado Júnior (Suplente) - Secretaria Especial de Administração

Carlos Augusto Pissutti (Titular); Bruno Pereira Pontes (Suplente) - Diretoria de Tecnologia

Kely Rejane de Almeida Romão Gonzaga - Coordenadora do Subcomitê de Segurança da Informação da Presidência da República.

**Equipe de Elaboração**

**Comissão de Proteção de Dados**

Edson Leonardo Dalescio Sá Teles (Titular); André Luiz Silva Lopes (Suplente) - Secretaria de Controle Interno/SG/PR (coordenação)

Claudir Afonso Costa (titular); Orlando Oliveira dos Santos (suplente) - Casa Civil

Vitor Poubel da Silva (titular); Ricardo de Assis Teixeira (suplente) - Secretaria de Governo

Jose Placidio Matias dos Santos (titular); Cel Gerson Vargas Ávila (suplente) - Gabinete de Segurança Institucional

Marcelo da Silva Vieira (titular); Erick Moutinho Borges (suplente) - Gabinete Pessoal do Presidente da República

Luiz Antonio Marques (titular); Silvia Antunes Ribeiro (suplente) - Secretaria Especial de Assuntos Estratégicos

Clovis Curado Júnior (titular); Humberto Miranda Cardoso (suplente) - Secretaria Especial de Administração/SG/PR

Israel Pinheiro Torres Junior (titular); Lia Meneleu Fiuza Favali (suplente) - Vice-Presidência

Carlos Augusto Pissutti (titular); Bruno Pereira Pontes (suplente) - Diretoria de Tecnologia (DITEC/SA/SG/PR)

Gustavo Andrade Bruzzeguez (titular); Kely Rejane de Almeida Romão Gonzaga (suplente) - Diretoria de Governança (DGO/SE/SG/PR)

**Colaboração**
Julianna Schimmelpfeng Pamplona de Moura Oliveira – Secretaria de Controle Interno/SG/PR
Silvana Stadniki Morato Miranda – Secretaria de Controle Interno/SG/PR
Rafaella Moisa Alvarenga – Secretaria de Controle Interno/SG/PR
Breiner Araujo Queiroz – Secretaria de Controle Interno/SG/PR
Valdir Campoi Junior – Secretaria de Controle Interno/SG/PR

# SUMÁRIO

# INTRODUÇÃO

A Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais – LGPD estabelece o regramento acerca da coleta, armazenamento, tratamento e compartilhamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

A LGPD é a primeira regulamentação abrangente de proteção de dados do Brasil e está amplamente alinhada à Lei Geral de Proteção de Dados da União Europeia (GDPR). Algumas disposições da LGPD já foram alteradas desde sua promulgação, incluindo o adiamento de sua aplicabilidade para agosto de 2020 e a criação da Autoridade Nacional de Proteção de Dados (ANPD). Antes da LGPD, as regulamentações de privacidade de dados no Brasil consistiam em várias disposições espalhadas pela legislação brasileira. Por exemplo, a Lei Federal nº. 12.965/2014 e seu Decreto regulamentar nº. 8.771/16 (em conjunto, a Lei Brasileira da Internet), que impõe alguns requisitos relativos à segurança e ao processamento de dados pessoais e outras obrigações aos provedores de serviços, provedores de redes e aplicativos, bem como direitos dos usuários da Internet.

As disposições e princípios gerais aplicáveis à proteção de dados também são encontrados na Constituição Federal; no Código Civil Brasileiro, e leis e regulamentos que tratam tipos específicos de relacionamentos (por exemplo, Código de Defesa do Consumidor e leis trabalhistas); setores específicos (por exemplo, instituições financeiras, indústria de saúde ou telecomunicações); e atividades profissionais específicas (por exemplo, medicina e direito). Além disso, existem leis sobre o tratamento e salvaguarda de documentos e informações tratados por entidades governamentais e órgãos públicos.

A LGPD, para resguardar direitos dos titulares dos dados, impôs o cumprimento de diversas obrigações às instituições, que precisam estar preparadas para atender, dentro de um prazo razoável, as exigências da nova lei brasileira. A adequação dos órgãos e entidades em relação à LGPD envolve uma transformação cultural que deve alcançar os níveis estratégico, tático e operacional da instituição. Sua aplicação deve acontecer em qualquer operação de tratamento efetuada por pessoa singular ou coletiva, de direito público ou privado, independentemente do meio utilizado para o tratamento, do país onde se encontra a sua sede ou do país onde se encontram os dados, desde que: a operação de processamento seja realizada no Brasil; o objetivo da atividade de processamento seja a oferta ou prestação de bens ou serviços, ou o processamento de dados de pessoas físicas localizadas no Brasil; ou os dados pessoais tenham sido coletados no Brasil.

Por outro lado, a lei não se aplica ao tratamento de dados pessoais que seja realizado por pessoa física exclusivamente para fins privados e não econômicos; realizado para fins jornalísticos, artísticos ou acadêmicos; realizado para fins de segurança pública, segurança nacional e defesa ou atividades de investigação e repressão de infrações penais (que serão objeto de lei específica); ou originados fora do território brasileiro e não são objeto de comunicação; uso de dados compartilhados com agentes de processamento brasileiros ou objeto de transferência internacional de dados com outro país que não seja o país de origem, desde que o país de origem ofereça um nível de proteção de dados pessoais adequado ao estabelecido na legislação brasileira.

No intuito de estabelecer uma metodologia de adequação e conformidade da Presidência da República com os requisitos da Lei Geral de Proteção de Dados para realizar tal transformação, o Comitê de Governança Digital da Presidência da República – CGD/PR, por meio da Resolução nº 1, de 14 de janeiro de 2021, constituiu Grupo de Trabalho composto por servidores representantes dos órgãos integrantes da Presidência da República: Secretaria-Geral, Casa

Civil, Secretaria de Governo, Gabinete de Segurança Institucional, Gabinete Pessoal do Presidente da República, Secretaria Especial de Assuntos Estratégicos e da Vice-Presidência da República.

O trabalho resultou na confecção de relatório contendo as etapas e ações necessárias para a elaboração do Plano de Proteção de Dados da Presidência da República. O relatório foi aprovado pelo CGD/PR que, na sequência, instituiu o Programa de Governança em Privacidade da Presidência da República e criou a Comissão de Proteção de Dados da Presidência da República, por meio das Resoluções CGD/PR nº 8 e 9, de 2 de setembro de 2021.

Como entrega resultante de suas atividades, a Comissão de Proteção de Dados da PR apresenta este Plano de Proteção de Dados, contendo as ações definidas para a adequação da Lei Geral de Proteção de Dados na Presidência da República, em conformidade com o art. 3º da supracitada Resolução CGD/PR nº 9/2021.

# PLANO DE PROTEÇÃO DE DADOS DA PRESIDÊNCIA DA REPÚBLICA

Este plano refere-se à implantação de processos que adequem ou ajustem mecanismos de coleta, tratamento e utilização de dados pessoais, com o intuito de que haja transparência absoluta nesses procedimentos, considerando o direito do titular do dado pessoal em saber de que forma o mesmo está armazenado e as finalidades para as quais esta providência foi tomada.

### Elaboração da proposta

Diante disso, considerando que a adequação à LGPD consiste em um processo de médio a longo prazo, definiu-se como melhor estratégia a abordagem por ação, subdividida em fases, conforme detalhado a seguir.

### AÇÃO 1: CAMPANHA DE CONSCIENTIZAÇÃO

Com objetivo de mobilizar a atenção dos servidores para a importância do assunto, serão realizadas ações para conscientização das etapas de adequação da LGPD na Presidência da República, com a finalidade de disseminar conteúdos e materiais, a fim de prepará-los para a execução das atividades que deverão ser desenvolvidas, além de fomentar o respeito à privacidade dos dados pessoais, que deverá ser adotado não apenas na implementação do plano, mas nas atividades executadas cotidianamente por todas as unidades da Presidência da República e pela Vice-Presidência da República.

## AÇÃO 2: DIAGNÓSTICO DAS NECESSIDADES DE ADEQUAÇÃO DA PR À LGPD

Esta etapa busca compreender quais são as primeiras informações e os dados importantes que devem ser conhecidos para identificar o atual estágio de adequação à LGPD.

### 2.1 Abordagem adotada para o diagnóstico

Para a realização do diagnóstico, será utilizado o questionário disponibilizado pela Secretaria de Governo Digital do Ministério da Economia (SGD/ME), que tem como intuito fornecer ao órgão respondente as informações necessárias para um diagnóstico do atual estágio de adequação à LGPD.

### 2.2 Resposta ao questionário da SGD do ME

O questionário encontra-se disponível através do link: https://www.gov.br/governodigital/pt-br/governanca-de-dados/diagnostico-de-adequacao-a-lgpd.

Insta consignar que houve por parte do Grupo de Trabalho constituído pela Resolução CGD/PR nº 1, de 14 de janeiro de 2021, durante a sua 7ª reunião, pauta para tratativas relacionadas à colaboração nas respostas que foram fornecidas pela Secretaria-Executiva da Casa Civil da Presidência da República ao Tribunal de Contas da União - TCU acerca de informações gerais sobre os controles implementados para adequação à LGPD.

### 2.3 Análise do questionário para obter um índice de maturidade

A partir do resultado do questionário da SGD/ME, mencionado no item anterior, será apresentado um índice de maturidade que possibilitará aos órgãos da Presidência da República e à Vice-Presidência

da República detectar as principais lacunas, indicando a direção dos esforços que deverão ser aplicados, bem como a priorização de ações que necessitam ser tomadas para sua adequação às obrigações presentes na LGPD, compondo assim o conjunto das medidas para adequação à legislação.

### 2.4 Identificação de instrumentos normativos

Feita tal avaliação, recomenda-se a identificação dos instrumentos normativos que regem a atuação dos órgãos da Presidência da República e da Vice-Presidência da República e que possuem relação com processos de Segurança da Informação e Privacidade cujas diretrizes possam ser aplicadas à proteção de dados pessoais.

### 2.5 Produção do relatório de recomendações para aderência e conformidade da PR à LGPD

Para realização das adequações, recomenda-se considerar todos os pontos do Guia de Boas Práticas editado pela SDG/ME, disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guia-boas-praticas-lgpd.

## AÇÃO 3: ELABORAÇÃO DE INVENTÁRIO DE DADOS PESSOAIS

O Inventário de Dados Pessoais – IDP consiste em catalogar informações fundamentais sobre o tratamento de dados pessoais na organização.

No inventário, deverão ser registradas informações sobre os processos de negócio que requerem tratamento de dados pessoais; o escopo, natureza e categoria dos dados pessoais envolvidos; a finalidade de seu uso; os agentes envolvidos no tratamento dos dados; as fases do ciclo de vida dos dados, entre outros elementos.

Para orientar esse processo nos órgãos da Administração Pública Federal, o Ministério da Economia desenvolveu o Guia Operacional para Inventário de Dados com orientações procedimentais e planilha modelo que indicam as informações básicas que podem compor esse inventário.

O material foi produzido inspirando-se em modelos adotados em países que estão mais avançados na temática de proteção de dados pessoais. O Guia está disponível no link: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_inventario_dados_pessoais.pdf.

### 3.1 Realização do inventário de dados de cada órgão da PR e VPR

Definido o modelo a ser considerado pelos órgãos da Presidência da República e Vice-Presidência da República para inventariar dados pessoais, cada órgão deve articular suas unidades para identificar os macroprocessos/serviços que passarão por esse nível de controle e levantar as informações necessárias.

O Guia de Elaboração de Inventário de Dados Pessoais produzido pelo Ministério da Economia sugere o modelo que envolve as seguintes fases:


Figura 1. Fases de elaboração do Inventário de Dados Pessoais.

Fonte: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guia_inventario_dados_pessoais.pdf

Nesta fase, deverá haver atuação ativa de coordenação e orientação por parte do membro da Comissão de Proteção de Dados, designado como responsável pela ação e sua equipe de apoio, para orientar os esforços e dirimir dúvidas dos agentes. Assim, haverá maior convergência na compreensão dos comandos necessários para preenchimento adequado das informações.

Uma recomendação do Grupo de Trabalho, constituído pela Resolução CGD/PR nº 1, de 14 de janeiro de 2021, foi de aproveitar a expertise de colaboradores que já atuem na condução de inventário de dados para efeito da Lei de Acesso à Informação (LAI). Embora representem inventários distintos, a habilidade prévia em atividades desta natureza pode favorecer o processo e, eventualmente, gerar algum nível de reaproveitamento de esforços.

### 3.2 Consolidação do inventário da Presidência da República

O Inventário de Dados Pessoais dos órgãos específicos da Presidência da República e Vice-Presidência da República, após consolidado, deverá compor repositório único para permitir a gestão do programa de privacidade.

### 3.3 Estabelecimento de processo de atualização do inventário

Tendo em vista que o Programa de Governança em Privacidade deve ser estabelecido e mantido de forma permanente no âmbito da Presidência da República, há necessidade de estabelecer processos sistemáticos e periódicos para atualização do inventário de dados pessoais.

Sem essa previsão, em poucos meses, os inventários poderão estar defasados, não retratando a situação real de uso de dados pessoais. Como é sabido, a dinâmica organizacional dos órgãos

palacianos possui natureza mais fluida e flexível que em outros órgãos governamentais.

Assim, o desenho processual a ser definido para execução das atividades de revisão deve considerar essa realidade, de forma que, a cada mudança de gestão, haja adequada revisão no quadro de responsáveis pelo tratamento de dados pessoais do respectivo setor. A delegação de competência será feita às unidades organizacionais e não às pessoas que as ocupam, de forma que as atribuições sejam automaticamente conferidas aos ocupantes sem necessidade de recorrentes revisões.

## AÇÃO 4: ELABORAÇÃO DE TERMO DE USO E POLÍTICA DE PRIVACIDADE

Termo de Uso ou contrato de Termo de Uso é um documento que estabelece as regras e condições de uso de determinado serviço. Caso o Termo de Uso seja aceito pelo usuário, a utilização do serviço será vinculada às cláusulas dispostas nele. Já a Política de Privacidade é um documento informativo pelo qual o prestador de serviço transparece ao usuário a forma como o serviço realiza o tratamento dos dados pessoais e como ele fornece privacidade ao usuário.

Tanto o Termo de Uso quanto a Política de Privacidade originam-se da responsabilidade de os agentes de tratamento de dados serem transparentes com o titular de dados e informarem como as atividades de tratamento de dados atendem os princípios dispostos no art. 6º da Lei Geral de Proteção de Dados (LGPD). Portanto, os dois documentos constituem, ao mesmo tempo, um dever do controlador e um direito do titular.

### 4.1 Elaboração de Política de Privacidade

Para a elaboração da Política de Privacidade, é fundamental entender o contexto do tratamento de dados pessoais e como os princípios da LGPD são atendidos no sistema ou serviço. Para tanto, é necessário mapear todos os dados pessoais, a

finalidade, as bases legais que legitimam o tratamento e a forma de atendimento aos direitos do titular como acesso, retificação, exclusão, revogação de consentimento, oposição, informação sobre possíveis compartilhamentos com terceiros e portabilidade.

A Política de Privacidade é única e orientada ao serviço e à organização responsável, inclusive no que tange à linguagem utilizada, algumas mais formais, outras informais. Não importa a forma, é preciso garantir que o conteúdo seja conciso, de fácil acesso e compreensão. Utilizar aspectos visuais, como vídeos e imagens, pode ser um bom instrumento para facilitar o entendimento da política.

### 4.2 Revisão e aprovação da Política de Privacidade

Para a devida aprovação da Política de Privacidade, é essencial que a área jurídica esteja inserida no processo e revise a minuta do documento.

### 4.3 Elaboração do Termo de Uso para processos/serviços/sistemas que tratam dados pessoais

O item refere-se a Termo de Uso e Política de Privacidade vinculados à utilização de serviços públicos por meio de aplicações (sítios, sistemas ou aplicativos para dispositivos móveis) fornecidas por órgãos e entidades da Administração Pública.

Com relação ao conteúdo, é importante observar a presença de pelo menos as seguintes informações, que devem estar de modo claro e preciso:

- Informações sobre a organização responsável pelo tratamento;
- Dados pessoais e respectivas finalidades do tratamento, inclusive os dados não informados pelo usuário (exemplo: IP, localização, etc);

- Base jurídica do tratamento;
- Prazo de retenção dos dados pessoais; e
- Informações de contato do encarregado de proteção de dados da Presidência da República.

A Política de Privacidade também deve orientar como são atendidos os direitos do titular de dados pessoais, apresentando como ele pode acessar, retificar, solicitar a exclusão de dados, transferir, limitar ou se opor ao tratamento e retirar o consentimento. No caso da inviabilidade de alguma operação, é necessário deixar claro o motivo. Entretanto, aconselha-se que esses casos sejam avaliados e autorizados pela área jurídica, sendo justificados por algum outro requisito legal.

Já o Termo de Uso deve evidenciar de forma clara quais são as responsabilidades de cada parte envolvida no serviço. Ao definir responsabilidades, a Administração Pública e o cidadão estabelecem direitos e deveres para ambas as partes e compreendem suas obrigações ao utilizar e prover o serviço, de forma a esclarecer quais situações configuram violações aos termos e para quais situações cabem reparação de danos.

Detalhes do que deve conter no Termo de Uso e Política de Privacidade para serviços públicos constam no guia disponibilizado pelo Ministério da Economia, por meio da Secretaria Especial de Desburocratização, Gestão e Governo Digital, disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_tupp.pdf.

Identificou-se ainda que há uma ferramenta ainda em fase de teste desenvolvida pela Secretaria de Governo Digital por meio da qual os órgãos e entidades da Administração Pública poderão, ao responder um questionário sobre informações relacionadas aos tópicos presentes no guia de elaboração, obter o texto completo de um modelo de termo de uso e política de privacidade. Tal ferramenta encontra-se disponível através do link: https://pesquisa.sisp.gov.br/index.php/759958?lang=pt-BR

### 4.4 Implementação do Termo de Uso e Política de Privacidade

A Política de Privacidade será disponibilizada ao titular dos dados antes do início do tratamento do dado pessoal dele, permitindo, quando aplicável, que o mesmo avalie os termos do site ou serviço.

É importante garantir que a política esteja facilmente disponível, em uma linguagem apropriada ao seu público-alvo e com o conteúdo suficiente, claro e preciso para declarar todas as informações necessárias. Dessa forma, a organização demonstra profissionalmente seu compromisso com a transparência no tratamento dos dados pessoais. E o usuário deve demonstrar seu expresso consentimento e concordância com os termos da política antes do início desse tratamento.

## AÇÃO 5: ANÁLISE DE RISCO DE SEGURANÇA DE PRIVACIDADE

A autorização para tratamento de dados impõe uma série de obrigações com o objetivo de proteger os titulares dos dados, e dentre essas obrigações está a de identificar eventuais riscos decorrentes do tratamento, com a consequente previsão de medidas que são adotadas para minimizar esses riscos.

A identificação, análise e previsão de medidas para tratamento dos riscos constitui concretização dos princípios da segurança e prevenção previstos na LGPD, já que irão permitir a utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão (art. 6º, VII) e a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais (art. 6º, VIII).

Tais medidas irão fazer parte do relatório de impacto à proteção de dados pessoais (art. 5º, XVII), conforme será abordado adiante.

Para a realização da ação, é importante a consulta do Guia de Avaliação de Riscos de Segurança e Privacidade disponibilizado pela Secretaria de Governo Digital em

https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_avaliacao_riscos.pdf, inclusive para definição do método de avaliação que será adotado, devendo ser observado ainda a Política de Gestão de Riscos.

### 5.1 Identificação dos riscos de segurança e privacidade de dados pessoais

A partir dos dados inventariados, devem ser identificados os riscos de segurança e privacidade.

### 5.2 Análise e classificação dos riscos

Identificados os riscos, devem ser realizadas a análise e classificação, com utilização de parâmetros sobre probabilidade de ocorrência e impacto: baixo, moderado e alto, que permitirão a classificação posterior (baixo risco, médio risco, alto risco).

### 5.3 Tratamento dos riscos

Identificar as medidas, sejam de segurança, técnicas ou administrativas e controles que serão adotados em cada situação identificada, implementando as medidas para evitar a ocorrência dos riscos ou adotando medidas de gerenciamento, no caso de ocorrência.

### 5.4 Monitoramento dos riscos

Acompanhamento da implementação das medidas de tratamento de riscos, identificando o surgimento de novos riscos ou a necessidade de revisão das medidas de tratamento.

### 5.5 Consolidação de análise de riscos de segurança e privacidade de toda a PR

A consolidação de análise de riscos de segurança e privacidade será realizada de forma colaborativa entre os membros da Comissão de Proteção de Dados.

## AÇÃO 6: ADEQUAÇÃO DE CONTRATOS ADMINISTRATIVOS E INSTRUMENTOS CONGÊNERES

Para adaptar os contratos, convênios e outros instrumentos que impliquem no tratamento de dados pessoais mapeados pelo Inventário, os modelos e documentos vigentes devem ser revistos.

O levantamento dos serviços que tratam dados pessoais no Inventário de Dados viabiliza a realização de uma correlação com os contratos que os suportam. Esse mapeamento dos contratos, que coletam, transferem e processam dados pessoais, contribui para possíveis e necessárias adequações, tanto nos contratos existentes quanto nos futuros.

## AÇÃO 7: RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

O Relatório de Impacto à Proteção de Dados Pessoais (RIPD) representa documento fundamental a fim de demonstrar que o controlador realizou uma avaliação de riscos nas operações de tratamento dos dados pessoais que são coletados, tratados, processados, compartilhados e quais medidas são adotadas para mitigação dos riscos que possam afetar as liberdades civis e direitos fundamentais dos titulares desses dados (art. 5°, inciso XVII, da Lei Geral de Proteção de Dados).

O art. 38 da Lei Geral de Proteção de Dados estabelece que "autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos

comercial e industrial". Dispõe o parágrafo único do referido artigo que o relatório deverá conter a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

### 7.1 Elaboração, revisão e aprovação de relatórios de impactos e proteção de dados

O RIPD deve ser elaborado, preferencialmente, antes de a instituição iniciar o tratamento de dados pessoais.

A elaboração contempla as seguintes etapas:

1. Identificar os Agentes de Tratamento e o Encarregado;
2. Identificar a necessidade de elaborar o Relatório;
3. Descrever o tratamento;
4. Identificar partes interessadas consultadas;
5. Descrever necessidade e proporcionalidade;
6. Identificar e avaliar os riscos;
7. Identificar medidas para tratar os riscos;
8. Aprovar o Relatório; e
9. Manter revisão.

**Nota:** O Guia de Boas Práticas – Lei Geral de Proteção de Dados publicado pelo Comitê Central de Governança de Dados – agosto de 2019 – disponibiliza modelo de RIPD em seu Anexo I.

### 7.2 Identificação dos Agentes de Tratamento e o Encarregado

Esta etapa consiste em identificar os agentes de tratamento (controlador e operador) e o encarregado no RIPD (art. 5º da LGPD). Esses atores desempenham papel essencial no levantamento das informações necessárias para elaboração do RIPD.

> *Art. 5º Para os fins desta Lei, considera-se:*
>
> *VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;*
> *VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;*
>
> *VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); (Redação dada pela Lei nº 13.853, de 2019).*
>
> *A conclusão desta etapa envolve registrar o e-mail e o telefone de contato do encarregado, já que ele é o canal de comunicação entre o controlador, titulares dos dados e ANPD.*

### 7.3 Identificação da necessidade de elaborar o Relatório

Inicialmente, é fundamental conhecer os casos específicos previstos pela LGPD em que o RIPD deverá ou poderá ser solicitado. São eles:

- Para tratamento de dados pessoais realizados para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (exceções previstas pelo inciso III, do art. 4º);
- Quando houver infração da LGPD em decorrência do tratamento de dados pessoais por órgãos públicos (arts. 31 e 32 combinados); e
- A qualquer momento sob determinação da ANPD (art. 38).

Quando for necessária a elaboração do RIPD, a instituição deve avaliar se os programas, sistemas de informação ou processos existentes ou a serem implementados geram impactos à proteção dos dados pessoais, a fim de decidir sobre a elaboração ou atualização do RIPD.

A elaboração de um único RIPD para todas as operações de tratamento de dados pessoais ou de um RIPD para cada projeto, sistema ou serviço deve ser avaliada por cada instituição de acordo com os processos internos de trabalho. Assim, uma instituição que realiza tratamento de quantidade reduzida de dados pessoais, com poucos processos e serviços, pode optar por um RIPD único. Já uma instituição que implementa vários processos, projetos, sistemas e serviços que envolvam o tratamento de expressiva quantidade e diversidade de dados pessoais pode considerar que a elaboração de um único RIPD não seja a opção mais indicada, optando por elaborar RIPDs segregados, por ser mais adequado à sua realidade.

Além dos casos específicos previstos pela LGPD, é indicada a elaboração ou atualização do Relatório de Impacto sempre que existir a possibilidade de ocorrer impacto na privacidade dos dados pessoais, resultante de:

• uma tecnologia, serviço ou outra nova iniciativa em que dados pessoais e dados pessoais sensíveis sejam ou devam ser tratados;

• rastreamento da localização dos indivíduos ou qualquer outra ação de tratamento que vise a formação de perfil comportamental de pessoa natural, se identificada (LGPD, art. 12, § 2º);

• tratamento de dado pessoal sobre "origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (LGPD, art. 5º, II);

• processamento de dados pessoais usado para tomar decisões automatizadas que possam ter efeitos legais, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade (LGPD, art. 20);

• tratamento de dados pessoais de crianças e adolescentes (LGPD, art. 14);

• tratamento de dados que possa resultar em algum tipo de dano patrimonial, moral, individual ou coletivo aos titulares de dados, se houver vazamento (LGPD, art. 42);

• tratamento de dados pessoais realizados para fins exclusivos de segurança pública, defesa nacional, segurança do Estado, ou atividades de investigação e repressão de infrações penais (LGPD, art. 4º, § 3º);

• tratamento no interesse legítimo do controlador (LGPD, art. 10, § 3º);

• alterações nas leis e regulamentos aplicáveis à privacidade, política e normas internas, operação do sistema de informações, propósitos e meios para tratar dados, fluxos de dados novos ou alterados etc; e

• reformas administrativas que implicam em nova estrutura organizacional resultante da incorporação, fusão ou cisão de órgãos ou entidades.

Em síntese, nesta etapa deve(m) ser explicitado(s) qual(is) dos itens elencados acima expressa(m) a necessidade de o RIPD ser elaborado ou atualizado pela instituição.

### 7.4 Descrição do tratamento

A descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais envolve a especificação da natureza, escopo, contexto e finalidade do tratamento.

Lembrando que a LGPD (art. 5º, X) considera tratamento "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração".

O objetivo principal desta descrição é fornecer cenário institucional relativo aos processos que envolvem o tratamento dos dados pessoais, fornecendo subsídios para avaliação e tratamento de riscos.

Caso a instituição considere mais adequado para sua realidade de tratamento de dados pessoais, pode-se sintetizar a natureza, escopo, contexto e finalidade do tratamento em uma única seção do RIPD, sem necessidade de segregar a descrição do tratamento em subseções.

### 7.5 Natureza do tratamento

A natureza representa como a instituição pretende tratar ou trata o dado pessoal.

Importante descrever, por exemplo:

- como os dados pessoais são coletados, retidos/armazenados, tratados, usados e eliminados;
- fonte de dados (ex: titular de dados, planilha eletrônica, arquivo .xml, formulário em papel etc.) utilizada para coleta dos dados pessoais;
- com quais órgãos, entidades ou empresas os dados pessoais serão compartilhados;
- quais são os operadores que realizam o tratamento de dados pessoais em nome do controlador e destacar em quais fases (coleta, retenção, processamento, compartilhamento, eliminação) eles atuam;
- se adotou recentemente algum tipo de nova tecnologia ou método de tratamento que envolva dados pessoais. A informação sobre o uso de nova tecnologia ou método de tratamento é importante no sentido de possibilitar a identificação de possíveis riscos resultantes de tal uso; e
- medidas de segurança atualmente adotadas.

Na elaboração dessa descrição, é importante considerar a possibilidade de consultar um diagrama ou qualquer outra documentação que demonstre os fluxos de dados da instituição.

### 7.6 Escopo do tratamento

O escopo representa a abrangência do tratamento de dados. Nesse sentido, é importante considerar:

- as informações sobre os tipos dos dados pessoais tratados, ressaltando quais são considerados dados pessoais sensíveis;
- o volume dos dados pessoais a serem coletados e tratados;
- a extensão e frequência em que os dados são tratados;

• o período de retenção, informação sobre quanto tempo os dados pessoais serão mantidos, retidos ou armazenados;

• o número de titulares de dados afetados pelo tratamento; e

• a abrangência da área geográfica do tratamento.

O levantamento das informações elencadas acima auxilia a determinar se o tratamento de dados pessoais é realizado em alta escala.

### 7.7 Contexto do tratamento

Nesta etapa, convém destacar um cenário mais amplo, incluindo fatores internos e externos que podem afetar as expectativas do titular dos dados pessoais ou o impacto sobre o tratamento dos dados.

O levantamento das informações destacadas abaixo proporciona a obtenção de parâmetros que permitirão demonstrar o equilíbrio entre o interesse e a necessidade do controlador em tratar os dados pessoais e os direitos dos titulares de tais dados:

• natureza do relacionamento da organização com os indivíduos;

• nível ou método de controle que os indivíduos exercem sobre os dados pessoais;

• destacar se o tratamento envolve crianças, adolescentes ou outro grupo vulnerável;

• destacar se o tipo de tratamento realizado sobre os dados é condizente com a expectativa dos titulares dos dados pessoais. Ou seja, o dado pessoal não é tratado de maneira diversa do que é determinado em leis e regulamentos, e comunicado pela instituição ao titular de dados;

• destaque de qualquer experiência anterior com esse tipo de tratamento de dados; e

• destaque de avanços relevantes da instituição em tecnologia ou segurança que contribuem para a proteção dos dados pessoais.

### 7.8 Finalidade do tratamento

A finalidade é a razão ou motivo pelo qual se deseja tratar os dados pessoais. É importantíssimo estabelecer claramente a finalidade, pois é ela que justifica o tratamento e fornece os elementos para informar o titular dos dados.

Nesta etapa, é importante detalhar o que se pretende alcançar com o tratamento dos dados pessoais, considerando os exemplos de finalidades elencadas abaixo, embasados nos arts. 7º e 11 da LGPD, no que for aplicável:

- cumprimento de obrigação legal ou regulatória pelo controlador;
- execução de políticas públicas;
- alguma espécie de estudo realizado por órgão de pesquisa;
- execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
- exercício regular de direitos em processo judicial, administrativo ou arbitral;
- proteção da vida ou da incolumidade física do titular ou de terceiro;
- tutela da saúde;
- atender aos interesses legítimos do controlador ou de terceiro;
- proteção do crédito; e
- garantia da prevenção à fraude e à segurança do titular.

Cumpre destacar que os exemplos de finalidades apresentados no presente relatório não são exaustivos. Desse modo, deve-se informar e detalhar qualquer outra finalidade específica do controlador para tratamento dos dados pessoais.

Ao detalhar a finalidade do tratamento dos dados pessoais, é importante:

• Indicar qual(is) o(s) resultado(s) pretendido(s) para os titulares dos dados pessoais, informando o quão importantes são esses resultados; e

• Informar os benefícios esperados para o órgão, entidade ou para a sociedade como um todo.

Neste momento, deve-se atentar para o caso de a finalidade ser para atender o legítimo interesse do controlador. Nesse caso, somente poderá ser fundamentado tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, conforme previsto pelo art. 10 da LGPD.

> *Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:*
>
> *I - apoio e promoção de atividades do controlador; e*
> *II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.*
>
> *§ 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.*
> *§ 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.*
>
> *§ 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de*

*dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.*

Cumpre ressaltar que a instituição deve equilibrar seus interesses com os dos indivíduos com os quais ela tem relacionamento.

### 7.9 Identificação das partes interessadas consultadas

Partes interessadas relevantes, internas e externas, consultadas a fim de obter opiniões legais, técnicas ou administrativas sobre os dados pessoais que são objeto do tratamento.

Nesta etapa, é importante identificar:

- quais partes foram consultadas, como, por exemplo: operador (LGPD, art. 5º, VII), encarregado (LGPD, art. 5º, VIII), gestores, especialistas em segurança da informação, consultores jurídicos etc.; e
- o que cada parte consultada indicou como importante a ser observado para o tratamento dos dados pessoais em relação aos possíveis riscos referentes às atividades de tratamento em análise. Também deve-se observar os riscos de não-conformidade ante a LGPD e os instrumentos internos de controle (políticas, processos e procedimentos voltados à proteção de dados e privacidade).

Caso não seja conveniente registrar o que foi consultado, então é importante apresentar o motivo de não ter realizado tal registro. Como, por exemplo, apresentar justificativa de que informar o registro das opiniões das partes internas comprometeria segredo comercial ou industrial; fragilizaria a segurança da informação; ou seria desproporcional ou impraticável realizar o registro das opiniões obtidas.

### 7.10 Descrição da necessidade e proporcionalidade

Descrever como a instituição avalia a necessidade e proporcionalidade dos dados. É necessário demonstrar que as operações realizadas sobre os dados pessoais limitam o tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados (LGPD, art. 6º, III).

Nesse sentido, destacar:

• A fundamentação legal para o tratamento dos dados pessoais;

• Caso o fundamento legal seja embasado no legítimo interesse do controlador (LGPD, art. 10), demonstrar que:

- esse tratamento de dados pessoais é indispensável;

- não há outra base legal possível de se utilizar para alcançar o mesmo propósito; e

- esse processamento de fato auxilia no propósito almejado.

• Como será garantida a qualidade (exatidão, clareza, relevância e atualização dos dados) e minimização dos dados;

• Quais medidas são adotadas a fim de assegurar que o operador (LGPD, art. 5º, VII) realize o tratamento de dados pessoais, conforme a LGPD e respeite os critérios estabelecidos pela instituição que exerce o papel de controlador (LGPD, art. 5º, VI);

• Como estão implementadas as medidas que asseguram o direito do titular dos dados pessoais obter do controlador o previsto pelo art. 18 da LGPD;

• Como a instituição pretende fornecer informações de privacidade para os titulares dos dados pessoais; e

• Quais são as salvaguardas para as transferências internacionais de dados.

O art. 18 da LGPD é bem extenso e trata do direito que o titular tem de requisitar do controlador ações e informações específicas em relação ao tratamento realizado sobre os dados pessoais.

### 7.11 Identificação e avaliação dos riscos

O art. 5º, XVII, da LGPD preconiza que o Relatório de Impacto deve descrever "medidas, salvaguardas e mecanismos de mitigação de risco".

Antes de definir tais medidas, salvaguardas e mecanismos, é necessário identificar os riscos que geram impacto potencial sobre o titular dos dados pessoais.

Para cada risco identificado, define-se: a probabilidade de ocorrência do evento de risco, o possível impacto caso o risco ocorra, avaliando o nível potencial de risco para cada evento.

Parâmetros escalares podem ser utilizados para representar os níveis de probabilidade e impacto que, após a multiplicação, resultarão nos níveis de risco, que direcionarão a aplicação de medidas de segurança. Informações detalhadas sobre riscos de privacidades podem ser obtidas na norma ISO/IEC 29134:2017 seção 6.4.4.

Importante destacar que o gerenciamento de riscos relacionado ao tratamento dos dados pessoais deve ser realizado em harmonia com a Política de Gestão de Riscos do órgão preconizada pela Instrução Normativa Conjunta MP/CGU nº 1, de 10 de maio de 2016.

### 7.12 Identificação das medidas para tratar os riscos

Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (LGPD, art. 46).

Importante reforçar que as medidas para tratar os riscos podem ser: de segurança, técnicas ou administrativas.

A instituição nem sempre precisa eliminar todos os riscos. Nesse sentido, pode-se decidir que alguns riscos são aceitáveis,

até um risco de nível alto, devido aos benefícios do processamento dos dados pessoais e dificuldades de mitigação. No entanto, se houver um risco residual de nível alto, é recomendável consultar a ANPD antes de prosseguir com as operações de tratamento dos dados pessoais.

### 7.13 Aprovação do relatório

Esta etapa visa formalizar a aprovação do RIPD por meio da obtenção das assinaturas do responsável pela elaboração do RIPD, pelo encarregado e pelas autoridades que representam o controlador e operador.

O responsável pela elaboração do Relatório pode ser o próprio encarregado ou qualquer outra pessoa designada pelo controlador com conhecimento necessário para realizar tal tarefa.

### 7.14 Manutenção da revisão

O RIPD deve ser revisto e atualizado anualmente ou sempre que existir qualquer tipo de mudança que afete o tratamento dos dados pessoais realizados pela instituição.

De uma forma geral, essa mudança pode ser motivada por alteração:

- significativa na finalidade do tratamento de dados pessoais;
- que impacte no processo de como esses dados são tratados;
- expressiva na quantidade de dados pessoais coletados; e
- no contexto do tratamento de dados resultantes de identificação de falha de segurança, uso de uma nova tecnologia, nova preocupação pública sobre o tipo de tratamento de dados realizado pela instituição ou vulnerabilidade de um grupo específico de titulares de dados pessoais.

A instituição deve manter revisão do RIPD a fim de demonstrar que avalia continuamente os riscos de tratamento de dados pessoais que surgem em consequência do dinamismo das transformações nos cenários tecnológico, normativo, político e institucional.

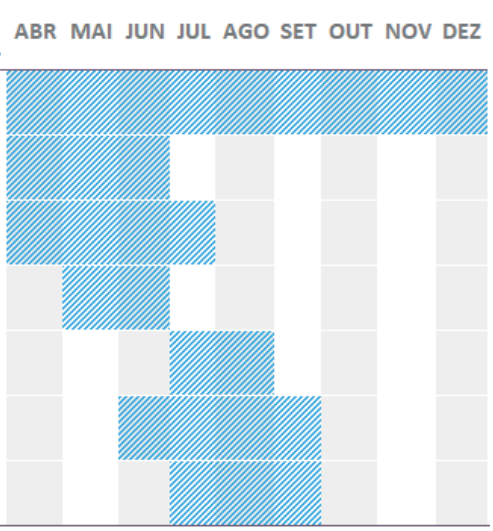
# CRONOGRAMA DE EXECUÇÃO

## Quadro 1: Ações, Metas e Responsáveis:

| | |
|---|---|
| **Ação 1: Campanha de Conscientização** | **Meta:** 1 (uma) campanha mensal |
| **Responsável pela Coordenação:** SA/SG/PR, Encarregado da PR e Encarregados Setoriais | |
| **Ação 2: Diagnóstico das necessidades de adequação da PR à LGPD** | **Meta:** questionários respondidos |
| **Responsável pela Coordenação:** a Comissão responderá conjuntamente | |
| **Ação 3: Elaboração de Inventário de Dados Pessoais** | **Meta:** formulários preenchidos |
| **Responsável pela Coordenação:** CISET/Casa Civil/ DITEC | |
| **Ação 4: Elaboração de Termo de Uso e Política de Privacidade** | **Meta:** Termo de Uso elaborado e política publicada |
| **Responsável pela Coordenação:** SEGOV | |
| **Ação 5: Análise de Risco de Segurança de Privacidade** | **Meta:** relatório concluído |
| **Responsável pela Coordenação:** GSI | |
| **Ação 6: Adequação de Contratos Administrativos e Instrumentos Congêneres** | **Meta:** contratos modificados |
| **Responsável pela Coordenação:** SA/SG/PR, com auxílio da DILOG/SA/SG/PR | |
| **Ação 7: Relatório de Impacto à Proteção de Dados** | **Meta:** relatório concluído |
| **Responsável pela Coordenação:** Encarregado da PR (CISET) e Encarregados Setoriais | |

## Quadro 2: Prazos para o cumprimento das ações no exercício 2022:

| AÇÕES | MÊS INICIAL | MÊS FINAL |
|---|---|---|
| Campanha de Conscientização | ABR | DEZ |
| Diagnóstico das Necessidades de Adequação da PR à LGPD | ABR | JUN |
| Elaboração de Inventário de Dados Pessoais | ABR | JUL |
| Elaboração de Termo de uso de Política de Privacidade | MAI | JUN |
| Análise de Risco de Segurança de Privacidade | JUL | AGO |
| Adequação de Contratos Administrativos e Instrumentos Congêneres | JUN | SET |
| Relatório de Impacto à Proteção de Dados Pessoais | JUL | SET |



Importante salientar que o cronograma de execução das ações poderá sofrer alterações em razão da complexidade técnica, que deverá ser empreendida nos processos de mudanças nos sistemas integrados da Presidência da República e Vice-Presidência da República. Ainda é necessário considerar a peculiaridade da estrutura da Presidência da República, que integra diversos órgãos e unidades de assistência direta ao Presidente da República, todos com especificidades próprias de atuação. Por fim, e não menos importante, registra-se o período de pandemia da covid, que pode comprometer, em certos momentos, a atuação dos servidores na execução deste Plano em suas respectivas unidades de lotação.

# REFERÊNCIAS


BRASIL. Lei n º 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm . Acesso em: 12 jan. 2022.

Guia de Boas Práticas para Implementação na Administração Pública Federal. Lei Geral de Proteção de Dados (LGPD). Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf . Acesso em: 6 jan. 2022.

Guia de Elaboração de Programa de Governança em Privacidade. Lei Geral de Proteção de Dados (LGPD). Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_governanca_privacidade.pdf . Acesso em: 11 jan. 2022.

Guia de Elaboração de Inventário de Dados Pessoais. Lei Geral de Proteção de Dados (LGPD). Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_inventario_dados_pessoais.pdf . Acesso em: 13 jan. 2022.

Guia de elaboração de Termo de Uso e Política de Privacidade para serviços públicos. Lei Geral de Proteção de Dados (LGPD). Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_tupp.pdf . Acesso em: 4 jan. 2022.

Guia de Avaliação de Riscos de Segurança e Privacidade. Lei Geral de Proteção de Dados (LGPD). Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_avaliacao_riscos.pdf . Acesso em: 7 jan. 2022.

Guia de Requisitos e de Obrigações quanto à Segurança da Informação e Privacidade. Lei Geral de Proteção de Dados (LGPD). Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_requisitos_obrigacoes.pdf . Acesso em: 7 jan. 2022.

Presidência da República. Comitê de Governança Digital e Segurança da Informação. Resolução nº 8, de 2 de setembro de 2021. Institui o Programa de Governança em Privacidade da Presidência da República. Disponível em: http://www4.planalto.gov.br/cgd/assuntos/legislacao/resolucoes/resolucao-no-8-de-02-de-setembro-de-2021 . Acesso em: 10 jan. 2022.

Presidência da República. Comitê de Governança Digital e Segurança da Informação. Resolução nº 9, de 2 de setembro de 2021. Dispõe sobre a criação da Comissão de Proteção de Dados da Presidência da República. Disponível em: http://www4.planalto.gov.br/cgd/assuntos/legislacao/resolucoes/resolucao-no-9-de-02-de-setembro-de-2021 . Acesso em: 10 jan. 2022.

COORDENAÇÃO-GERAL DE
**RELAÇÕES PÚBLICAS**

SECRETARIA ESPECIAL DE
**ADMINISTRAÇÃO**

CISET
Presidência da República

SECRETARIA-GERAL DA
**PRESIDÊNCIA DA REPÚBLICA**

PÁTRIA AMADA BRASIL
GOVERNO FEDERAL