MINISTÉRIO DA

DEFESA

BOLETIM DE PESSOAL E SERVIÇO - EDIÇÃO EXTRA Nº 42, DE 30 DE NOVEMBRO DE 2023

2. RESOLUÇÃO CGD-MD Nº 19, DE 21 DE NOVEMBRO DE 2023

Aprova o Programa de Gestão em Privacidade - PGP da administração central do Ministério da Defesa

O COMITÊ DE GOVERNANÇA DIGITAL DO MINISTÉRIO DA DEFESA - CGD-MD, no uso das atribuições que lhe confere o art. 7º, inciso II, da Portaria GM-MD nº 5.814, de 29 de novembro de 2022, tendo em vista o disposto no art. 3º, caput, e Objetivo 10 do Anexo do Decreto nº 10.332, de 28 de abril de 2020, no art. 6º, inciso VII, da Portaria GM-MD nº 3.572, de 29 de junho de 2022, e de acordo com o que consta nos Processos Administrativos nº 60586.000312/2022-25 e 60588.000003/2023-16, resolve:

Art. 1º Aprovar o Programa de Gestão em Privacidade - PGP da administração central do Ministério da Defesa, conforme deliberação de 29 de março de 2023, assentada em Ata da Reunião nº 136, do Comitê de Governança Digital da administração central do Ministério da Defesa - CGD-MD, na forma do anexo.

Parágrafo único. Esta Resolução e a íntegra do Programa de Gestão em Privacidade - PGP serão disponibilizados no sítio eletrônico do Ministério da Defesa (https://www.gov.br/defesa/pt-br/assuntos/legislacao) e na plataforma de pesquisa da legislação de Defesa - MDLegis (https://mdlegis.defesa.gov.br/pesquisar_normas).

Art. 2º Esta Resolução entra em vigor em 1 de dezembro de 2023.

BRUNO FASSHEBER NOVAIS

Departamento de Tecnologia da Informação e Comunicação

Secretaria de Orçamento e Organização Institucional da Secretaria-Geral
Presidente do CGD-MD

MARCELO MUCIOLO VIEIRA - Cel

Membro suplente

Gabinete do Estado-Maior Conjunto das Forças Armadas

C Alte SÉRGIO BLANCO OZÓRIO

Membro titular

Chefia de Assuntos Estratégicos do Estado-Maior Conjunto das Forças Armadas

CHARLES DE ESTEVAM DE OLIVEIRA HASLER - Cel R/1

Membro suplente

Gabinete da Secretaria-Geral

DANIEL SANTANA FERNANDES

Membro suplente

Secretaria de Produtos de Defesa da Secretaria-Geral

THIAGO D`AROLLA PEDROSA GALVÃO

Membro suplente

Departamento e Organização e Legislação

Secretaria de Orçamento e Organização Institucional da Secretaria-Geral

RENATA BITAR TIVERON

Membro titular

Centro Gestor e Operacional do Sistema de Proteção da Amazônia da Secretaria-Geral

LUIZ HENRIQUE CAVALCANTI DA SILVA

Membro titular

Encarregado pelo Tratamento de Dados Pessoais da administração central do MD

(Processo nº 60586.000312/2022-25)

WALDIR F. DAS N. SILVEIRA Jr
Diretor Substituto do Departamento de Administração Interna

Documento assinado eletronicamente por **WALDIR FRANCISCO DAS NEVES SILVEIRA JUNIOR**, **Diretor(a) Substituto(a)**, em 30/11/2023, às 16:05, conforme horário oficial de Brasília, com fundamento no § 3º, art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020 da Presidência da República.

A autenticidade do documento pode ser conferida no site https://sei.defesa.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, o código verificador **6746197** e o código CRC **F767054A**.

MINISTÉRIO DA
DEFESA

Comitê de Governança Digital

PROGRAMA DE

GESTÃO EM PRIVACIDADE

Brasília

1ª Edição - 2023

MINISTRO DE ESTADO DA DEFESA - MD
- José Mucio Monteiro Filho

CHEFE DO ESTADO-MAIOR CONJUNTO DAS FORÇAS ARMADAS - EMCFA

- Almirante de Esquadra Renato Rodrigues de Aguiar Freire

SECRETÁRIO GERAL - SG

- Luiz Henrique Pochyly da Costa

SECRETÁRIO DE ORÇAMENTO E ORGANIZAÇÃO INSTITUCIONAL - SEORI

- José Roberto de Moraes Rego Paiva Fernandes Júnior

DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - DETIC

- Bruno Fassheber Novais

RESPONSÁVEIS PELA ELABORAÇÃO DA PROGRAMA	
Membros da Assessoria Técnica – Tratamento de Dados Pessoais do Comitê de Governança Digital	Cel Inf (EB) Alexandre GUERRA Cel (EB) José FERNANDO Chagas Madeira CMG Ernesto RADEMAKER Martins Cel Inf R/1 SINVAL dos Reis Leite Cel R/1 (EB) RODRIGO Martins Prates CMG (RM1-T) MÁRCIA SOARES da Cunha Ten Cel Marcelo MULLER Pons Ten Cel (EB) Bráulio Fernando Ribeiro SAKAMOTO CF (T) ADALTO Pereira da Silva 1T (EB) Priscila Daniele PIVANTE 1º Ten QAO Edson JORGE do Santos SC LARISSE Cavalcante Lino Corrêa SC DANIEL Santana Fernandes SC Ivo BARBOSA Leite SC SHIGEAKI Ueki Homem do Brasil Alves dos Santos SC WARLEY Rodrigues de Almeida

ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS
- Luiz Henrique Cavalcanti da Silva

Sumário

LISTA DE TABELAS E FIGURAS

ABREVIATURAS, SIGLAS E ACRÔNIMOS

ANPD	Autoridade Nacional de Proteção de Dados
ASCOM	Assessoria Especial de Comunicação Social
ASPLAN	Assessoria Especial de Planejamento
CASLODE	Centro de Apoio à Sistemas Logísticos de Defesa
CENSIPAM	Centro Gestor e Operacional do Sistema de Proteção da Amazônia
CISET	Secretaria de Controle Interno
CONJUR	Consultoria Jurídica
DEADI/SEORI	Departamento de Administração Interna
DEORF/SEORI	Departamento de Planejamento, Orçamento e Finanças
DEORG/SEORI	Departamento de Organização e Legislação
DESEG/SEORI	Departamento de Engenharia e Serviços Gerais
DETIC/SEORI	Departamento de Tecnologia da Informação e Comunicação
EMCFA	Estado-Maior Conjunto das Forças Armadas
CHOC	Chefia de Operações Conjuntas
CAE	Chefia de Assuntos Estratégicos
CHEC	Chefia de Educação e Cultura
CHELOG	Chefia de Logística e Mobilização
ESG	Escola Superior de Guerra
ESD	Escola Superior de Defesa
LAI	Lei de Acesso à Informação
LGPD	Lei Geral de Proteção de Dados Pessoais
CGOVTI/DETIC	Coordenadora-Geral de Governança de Tecnologia da Informação
GM	Gabinete do Ministro
MD	Ministério da Defesa
OUV	Ouvidoria
SEORI	Secretaria de Orçamento e Organização Institucional
SEPESD	Secretaria de Pessoal, Ensino, Saúde e Desporto
SEPROD	Secretaria de Produtos de Defesa
SIC	Serviços de Informações ao Cidadão
TI	Tecnologia da Informação

Tabela 1. Abreviaturas, Siglas e Acrônimos

APRESENTAÇÃO

A Lei Geral de Proteção de Dados Pessoais - LGPD (Lei nº 13.709, de 14 de agosto de 2018), dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou 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.

Na administração pública, os preceitos da Lei Geral de Proteção de Dados Pessoais - LGPD estão alinhados com as ações que o Governo Brasileiro vem promovendo, em especial o incremento da transformação digital, a simplificação e ampliação da oferta de serviços públicos digitais aos cidadãos.

A Estratégia de Governo Digital - EGD, período 2020 a 2022, instituída pelo Decreto nº 10.332, de 28 de abril de 2020, orienta o assunto e elenca princípios, objetivos e iniciativas que norteiam a transformação do governo por meio de tecnologias digitais, de forma a oferecer políticas públicas e serviços de melhor qualidade, mais simples, acessíveis a qualquer hora e lugar e a um custo menor para o cidadão.

A Estratégia de Governo Digital - EGD contempla duas iniciativas voltadas para a implementação da Lei Geral de Proteção de Dados Pessoais - LGPD no âmbito do Governo Digital, que são coordenadas pela Secretaria de Governo Digital do Ministério da Economia:

> **Objetivo 10 - Implementação da Lei Geral de Proteção de Dados no âmbito do Governo federal**
> Iniciativa 10.1. Estabelecer método de adequação e conformidade dos órgãos com os requisitos da Lei Geral de Proteção de Dados, até 2020.
> Iniciativa 10.2. Estabelecer plataforma de gestão da privacidade e uso dos dados pessoais do cidadão, até 2020.

O referido Decreto estabeleceu, ainda, que os órgãos e as entidades da administração pública federal direta, autárquica e fundacional instituirão o Comitê de Governança Digital para deliberar sobre os assuntos relativos à implementação das ações de governo digital e ao uso de recursos de tecnologia da informação e comunicação.

No Ministério da Defesa, este Comitê teve sua instituição atualizada pela Portaria Normativa GM-MD nº 3.572, de 29 de junho de 2022, em cuja composição consta o Encarregado pelo tratamento de dados pessoais, conforme previsto no art. 2º, § 1º, inciso IV do referido Decreto nº 10.332, de 2020. Esta designação foi publicada por intermédio da Portaria GM-MD nº 1.648, de 9 de abril de 2021.

Com o propósito de propor a estrutura e as ações de Proteção de Dados Pessoais no âmbito da administração central do Ministério da Defesa, foi instituído um grupo de trabalho (Portaria GM-MD nº 5.148, de 14 de dezembro de 2021). Seu relatório final foi apresentado ao Comitê de Governança, em reunião extraordinária realizada em 31 de maio de 2022. Resultante do trabalho do Grupo de Trabalho, o Secretário-Geral orientou que fossem adotadas as providências para a adoção do Comitê de Governança Digital como estrutura de gestão da proteção de dados pessoais na administração central do Ministério da Defesa e para a implementação das ações propostas no Relatório Final do Grupo de Trabalho, visando incrementar a maturidade em proteção de dados pessoais.

No bojo dos trabalhos do Grupo de Trabalho, foi elaborada a Diretriz para a Proteção de Dados Pessoais no Ministério da Defesa, instituída pela Portaria GM-MD nº 5.814, de 29 de novembro de 2022 que norteia a conformidade com a Lei Geral de Proteção de Dados Pessoais - LGPD.

Cabe ressaltar que, conforme estabelecido no art. 13 da Estratégia de Governo Digital - EGD, os documentos de planejamento relacionados na tabela 1 foram revisados, visando sua adequação ao Decreto nº 10.332, de 2020, e aprovados pelo Comitê de Governança Digital.

Instrumento de Planejamento	Oficialização no âmbito do MD	Vigência
Plano de Transformação Digital (PTD)	Terceira repactuação, Documento 4858672, de 04/04/2022.	2020 a 2022
	Quarta repactuação em andamento Processo nº 60010.000168/2020-80	2023
Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC)	Portaria GM-MD nº 3.163, de 3 de junho de 2022 (2ª Revisão), Documento 5145800	2020 a 2023
Plano de Dados Abertos (PDA)	Portaria GM-MD nº 5.377, de 24 de outubro de 2022 (4ª Edição), Documento 5784894	2022 a 2024

Tabela 2. Instrumentos de Planejamento

Em continuidade às ações para adequar as operações de tratamento de dados pessoais realizadas pela administração central do Ministério da Defesa, o presente documento apresenta o Programa de Gestão em Privacidade - PGP, com o intuito de ser a base para a adoção de ações que assegurem o cumprimento, de forma abrangente, das normas e boas práticas relativas à proteção de dados pessoais na administração central do Ministério da Defesa.

1. INTRODUÇÃO

A Lei Geral de Proteção de Dados Pessoais - LGPD surgiu para atender a uma necessidade global de tratar dados pessoais de maneira mais segura e mitigar os riscos deste processo, visando garantir os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Em um contexto de transformação digital, no qual o Brasil busca ampliar cada vez mais a oferta de produtos, serviços e informações de governo por meio digital, é imperativo que se desenvolva e implemente medidas de segurança capazes de assegurar direitos constitucionais como a proteção de dados pessoais, a privacidade, a intimidade e a inviolabilidade da honra e da imagem das pessoas.

Assim, a Lei Geral de Proteção de Dados Pessoais - LGPD, inspirada nos preceitos do *General Data Protection Regulation* - GDPR, que regula a proteção de dados pessoais no âmbito da União Europeia, agregou novos conceitos ao arcabouço legal brasileiro, trazendo obrigações para a Administração Pública e fortalecendo os direitos dos titulares de dados pessoais.

Neste contexto, o dado é considerado pessoal quando permite a identificação, direta ou indireta, da pessoa à qual se refere. São exemplos de dados pessoais: nome; sobrenome; data de nascimento; número de inscrição no CPF, no RG, na CNH, número da carteira de trabalho, do passaporte e do título de eleitor; endereço residencial ou comercial; número de telefone; *cookies*; e endereço *IP*.

Além disso, a Lei Geral de Proteção de Dados Pessoais - LGPD confere proteção específica ao tratamento de dados pessoais sensíveis, ou seja, os dados pessoais relacionados à origem étnica ou racial, 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.

Cabe ressaltar que o dado, objeto da proteção prevista na Lei Geral de Proteção de Dados Pessoais - LGPD, deve ser visto não só isoladamente (dado pessoal propriamente dito), mas também dentro de seu contexto, visto que um dado que torne a pessoa identificável deve ser tratado à luz da Lei Geral de Proteção de Dados Pessoais - LGPD. Além dos conceitos estabelecidos na referida lei, o Decreto nº 10.046, de 9 de outubro de 2019, que dispõe sobre a governança no compartilhamento de dados na administração pública, agregou os termos atributos biográficos, atributos biométricos, dados cadastrais e atributos genéticos, permitindo assim uma classificação mais específica que contribui para a identificação dos dados pessoais no dia a dia.

Neste sentido, é imprescindível identificar os processos, manuais e digitais, que realizam tratamento de dados pessoais no âmbito do Ministério da Defesa, e realizar o inventário dos dados pessoais tratados, para identificar a finalidade do tratamento e permitir que sejam estabelecidos os métodos para adequação e conformidade aos preceitos da Lei Geral de Proteção de Dados Pessoais - LGPD. Ressalta-se a premência de realizar as ações de conformidade, visto que a Lei entrou em vigor em 18 de setembro de 2020 e suas sanções administrativas (arts. 52 a 54) são aplicáveis desde 1º de agosto de 2021.

Para tanto, é essencial que sejam identificados os agentes de tratamento de dados pessoais, conforme previsto na Lei Geral de Proteção de Dados Pessoais - LGPD, quais sejam:

a) Controlador: “pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais” (art. 5º, VI da LGPD). No caso das pessoas jurídicas de direito público, o Controlador é a União, mas, por força da desconcentração administrativa, as funções típicas de Controlador, além das obrigações legais, são atribuídas aos órgãos da administração pública; e

b) Operador: “pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador” (art. 5º, VII da LGPD), ou seja, o operador é aquele que realiza o tratamento de dados pessoais no limite das finalidades determinadas pelo Controlador (art. 39 da LGPD). Assim sendo, o operador será sempre uma pessoa distinta do órgão, não atuando como profissional subordinado ou membro do Controlador.

Sobre tais definições, a Diretriz para a Proteção de Dados Pessoais no Ministério da Defesa estabelece:

> Art. 2º O Ministério da Defesa exercerá as funções típicas de controlador, subsidiado, no que se refere à dimensão estratégica do assunto, pelo Comitê de Governança do Ministério da Defesa (CG-MD), instituído pela Portaria GM-MD nº 3.127, de 28 de julho de 2021.
>
> Art. 3º Os órgãos que integram o Ministério da Defesa deverão observar as disposições da Lei nº 13.709, de 2018, e aplicar os princípios previstos no seu art. 6º, em toda e qualquer operação de tratamento de dados pessoais que realizarem, independentemente do meio ou do país onde os dados estejam localizados.
>
> Parágrafo único. Deverão ser adotadas as diretrizes, os regulamentos, as normas, as orientações e os procedimentos expedidos pela Autoridade Nacional de Proteção de Dados Pessoais (ANPD), observadas as competências do art. 55-J da Lei nº 13.709, de 2018.
>
> [...]

Art. 5º O Comitê de Governança do Ministério da Defesa (CG-MD) acompanhará, em nível estratégico, as ações relacionadas ao tratamento de dados pessoais, por meio da estrutura de governança estabelecida, competindo-lhe:

I - apreciar propostas de diretrizes e políticas visando à conformidade com as disposições da Lei nº 13.709, de 2018;

II - promover e acompanhar a implementação de medidas e iniciativas para o incremento do nível de maturidade da proteção de dados pessoais;

III - fomentar a cultura de privacidade e proteção de dados pessoais; e

IV - propor aperfeiçoamentos na estrutura de governança estabelecida para o tratamento de dados pessoais.

Art. 6º A gestão das operações de proteção de dados pessoais será orientada e acompanhada:

I - no âmbito da administração central do MD, pelo Comitê de Governança Digital do Ministério da Defesa (CGD-MD); e

II - no âmbito do Hospital das Forças Armadas (HFA), da Escola Superior de Guerra (ESG), da Escola Superior de Defesa (ESD) e do Centro Gestor e Operacional do Sistema de Proteção da Amazônia (CENSIPAM), pelos respectivos comitês internos de governança ou instâncias equivalentes, os quais poderão estabelecer diretrizes e procedimentos complementares para o tratamento de dados pessoais em razão de suas especificidades.

Art. 7º Cabe ao CGD-MD e aos comitês internos de governança ou instância equivalentes do HFA, da ESG, da ESD e do CENSIPAM, no âmbito de suas competências:

I - subsidiar o CG-MD nos temas afetos à proteção de dados pessoais;

II - aprovar o Programa de Gestão em Privacidade (PGP), bem como suas revisões;

III - orientar e monitorar a implementação do PGP, acompanhando seus indicadores; e

IV - propor aperfeiçoamentos nas diretrizes, políticas, procedimentos e estruturas relacionados à proteção de dados pessoais.

Cabe destacar que a responsabilidade pelo cumprimento da Lei Geral de Proteção de Dados Pessoais - LGPD é do órgão como um todo, uma vez que as operações de tratamento de dados pessoais ocorrem rotineiramente na execução dos processos de trabalho da instituição, na concepção e execução de projetos, serviços ou produtos, no cumprimento de suas competências legais, no seu modelo de negócio e em sua cadeia de valor.

Devido ao fato do processo de adequação à Lei Geral de Proteção de Dados Pessoais - LGPD ter caráter multidisciplinar e multissetorial e impactar o órgão como um todo, se faz necessária a adoção de medidas sistêmicas que possam ser implementadas em toda organização. Tais medidas deverão considerar todas as fases do ciclo de vida do dado pessoal, a saber:

a) Coleta - Obtenção, recepção ou produção de dados pessoais independente do meio utilizado (documento físico, documento eletrônico, sistema de informação etc.);

b) Retenção - Arquivamento ou armazenamento de dados pessoais independente do meio utilizado (documento físico, documento eletrônico, banco de dados, arquivo de aço etc.);

c) Processamento - Qualquer operação que envolva classificação, utilização, reprodução, processamento, avaliação ou controle da informação, extração ou modificação de dados pessoais;

d) Compartilhamento - Qualquer operação que envolva transmissão, distribuição, comunicação, transferência, difusão e compartilhamento de dados pessoais; e

e) Eliminação - Qualquer operação que vise apagar ou eliminar dados pessoais. Esta fase também contempla o descarte dos ativos organizacionais, quando necessário.

Durante seu ciclo de vida, o dado pessoal é disponibilizado em um ou mais ativos organizacionais do Ministério da Defesa, tais como bases de dados, documentos, equipamentos, locais físicos, pessoas, sistemas e unidades organizacionais. Assim, é imprescindível relacionar os ativos que são utilizados durante todo o ciclo de vida do dado pessoal para que sejam implementadas as medidas de segurança e os respectivos controles necessários para a adequação da administração central do Ministério da Defesa à Lei Geral de Proteção de Dados Pessoais - LGPD.

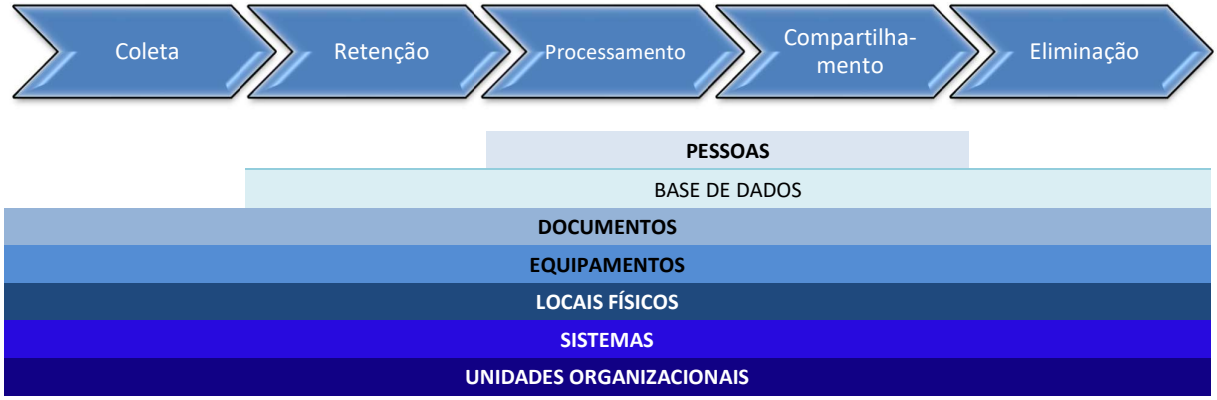

Figura 1. Ativos e fases do ciclo de vida dos dados pessoais

Nesse sentido, a elaboração de um Programa de Gestão em Privacidade - PGP possibilitará a captura e consolidação dos requisitos de privacidade com o intuito de definir como os dados pessoais serão manuseados durante todo o seu ciclo de vida.

2. OBJETIVOS

Este programa de gestão em privacidade tem por objetivos aperfeiçoar as operações de tratamento de dados pessoais e promover um ciclo de melhoria contínua para cumprir a legislação e normativos pertinentes, consolidando os requisitos de privacidade e proteção de dados pessoais no âmbito do Ministério da Defesa.

3. PROGRAMA DE GESTÃO EM PRIVACIDADE

O programa de gestão em privacidade consiste em um conjunto de atividades realizadas pelas diversas unidades organizacionais, à luz da Diretriz para Proteção de Dados Pessoais no Ministério da Defesa, para contribuir com a gestão dos dados pessoais durante todo seu ciclo de vida, mitigando os riscos inerentes.

Para tanto, a Diretriz estabelece que, considerando o volume e a natureza dos dados tratados, cada unidade organizacional deverá adotar, ao menos, as seguintes boas práticas:

a) mapear as atividades de tratamento e realizar o inventário dos dados pessoais tratados, mantendo-o atualizado;

b) elaborar o relatório de impacto à proteção de dados pessoais quando necessário;

c) adotar medidas de transparência aos usuários sobre o tratamento de dados pessoais, por meio do sítio institucional do Ministério da Defesa da internet;

d) fazer cumprir, no âmbito de suas atribuições e competências, a Política de Segurança da Informação;

e) determinar, no âmbito de suas atribuições e competências, que terceiros contratados estejam em conformidade com a Lei Geral de Proteção de Dados Pessoais - LGPD; e

f) incentivar a participação em eventos de capacitação, visando estimular a cultura de proteção de dados pessoais.

O processo de conformidade das operações de tratamento de dados pessoais, considerando as boas práticas acima relacionadas, deverá ser aprimorado constantemente mediante o emprego de um ciclo PDCA (*Plan, Do, Check e Act*), permitindo seu aperfeiçoamento e adequação à evolução do tema, em especial às regulamentações e orientações disseminadas pela Autoridade Nacional de Proteção de Dados - ANPD.

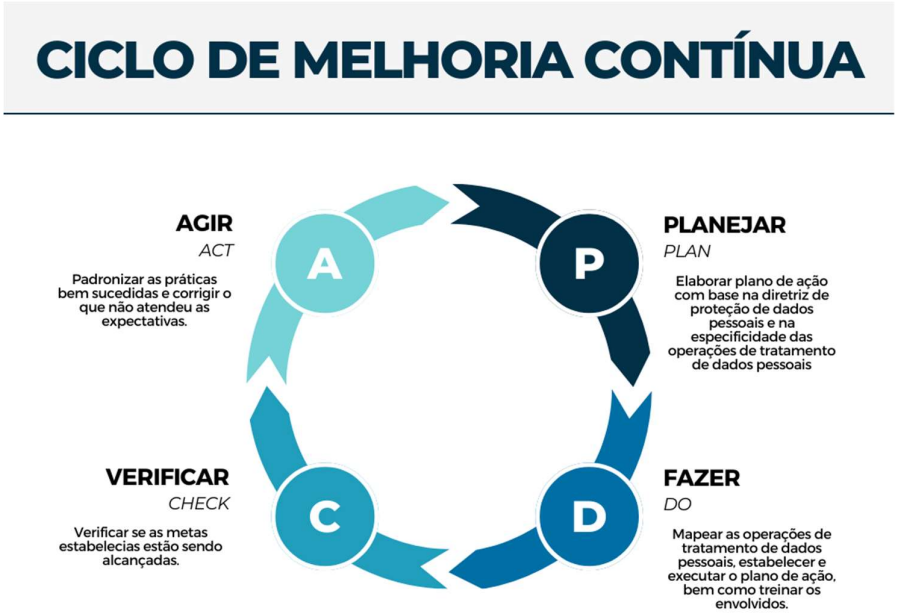

Figura 2. Ciclo PDCA

O Grupo de Trabalho instituído pela Portaria nº GM-MD nº 5.148, de 14 de dezembro de 2021, propôs ações de curto prazo (até dois anos) e de médio prazo (até quatro anos), a serem adotadas pelas unidades finalísticas e monitoradas por meio deste Programa de Gestão em Privacidade - PGP, as quais estão relacionadas na tabela a seguir.

Nº	Ação a empreender	Prazo	Coordenação
1	Implementar a estrutura de proteção de dados pessoais	curto	Comitê de Governança Digital
2	Publicar a Diretriz para a Proteção de Dados Pessoais	curto	
3	Instituir o Programa de Gestão em Privacidade (PGP)	curto	
4	Comunicar internamente os objetivos do PGP	curto	
5	Estabelecer um plano de comunicação no âmbito do PGP	curto	
6	Estabelecer e acompanhar indicadores no âmbito PGP	curto	

Nº	Ação a empreender	Prazo	Coordenação
7	Estabelecer procedimento para comunicar a Autoridade Nacional de Proteção de Dados e ao titular a ocorrência de incidentes de segurança que possa acarretar risco ou dano relevante aos titulares	curto	
8	Alocar recursos para a implementação de mecanismos para tratamento de dados pessoais	médio	
9	Avaliar se os dados pessoais são retidos apenas pelo tempo necessário para cumprir a finalidade do tratamento	médio	
10	Estabelecer medidas para assegurar que processos, serviços ou sistemas sejam projetados, desde a concepção e por padrão, em conformidade com a LGPD *(Privacy by Design* e *Privacy by default*)	médio	
11	Prover um canal para recebimento de denúncias e de alertas de ocorrência de irregularidades (Fala.br – externo e TI Ajudo - interno)	curto	Encarregado pelo tratamento de dados pessoais
12	Implementar sistema de gestão de consentimentos e exercício dos direitos dos titulares	médio	
13	Manter a designação do Encarregado pelo Tratamento de Dados Pessoais e seus dados de contato no sítio institucional do Ministério da Defesa	curto	Gabinete do Ministro
14	Incluir no Plano de Desenvolvimento de Pessoas da administração central do Ministério da Defesa cursos relacionados ao tratamento e proteção de dados pessoais	curto	DEADI
15	Atualizar a Política de Segurança da Informação	curto	Gestor de SI
16	Atualizar a Política de Classificação da Informação, incluindo a classificação de dados pessoais	curto	
17	Revisar e adequar contratos e outros instrumentos que prevejam o tratamento de dados pessoais	curto	Responsáveis por contratos
18	Identificar operadores que realizam tratamento de dados pessoais em nome do Ministério da Defesa e regularizar a situação contratual, se necessário	curto	
19	Realizar mapeamento e inventário de dados pessoais	curto	Unidades finalísticas que tratam dados pessoais
20	Identificar e documentar as finalidades e as bases legais das atividades de tratamento de dados pessoais	curto	
21	Avaliar se a coleta de dados é a estritamente necessária para a finalidade identificada	curto	
22	Identificar processos de negócio e responsáveis que realizam o tratamento de dados pessoais	curto	
23	Identificar categorias de titulares de dados pessoais com quem o órgão se relaciona	curto	
24	Implementar mecanismos para atender os direitos dos titulares de dados pessoais	curto	
25	Identificar os dados pessoais que são compartilhados com terceiros	curto	
26	Registrar eventos relacionados à transferência de dados pessoais que são compartilhados com terceiros	curto	
27	Identificar processos de transferência internacional de dados pessoais	curto	
28	Realizar inventário de serviços e sistemas que tratam dados pessoais	curto	
29	Classificar os dados tratados em dados pessoais e dados pessoais sensíveis	curto	
30	Monitorar vulnerabilidades técnicas nos sistemas e serviços que tratam dados pessoais, a fim de adequá-los às normas atinentes ao tema	curto	
31	Gerar evidências para comprovar que tomou medidas de segurança técnicas e administrativas para proteger os dados pessoais	curto	
32	Realizar gestão de incidentes para tratar possíveis violações dos dados pessoais	curto	

Nº	Ação a empreender	Prazo	Coordenação
33	Dar publicidade sobre a finalidade e a forma de tratamento de dados pessoais, por meio de termos de uso e aviso de privacidade ou divulgação na internet	curto	
34	Revisar e propor a atualização de manuais, normas, instruções e outros instrumentos que prevejam o tratamento de dados pessoais	curto	
35	Implementar processo formal para registro, cancelamento e provisionamento de usuários em sistemas que realizam o tratamento de dados pessoais	médio	
36	Manter rastreabilidade dos dados pessoais em meio físico e digital	médio	
37	Elaborar Relatório de Impacto à Proteção de Dados Pessoais (RIPD)	médio	
38	Implementar controles de segurança para riscos identificados no Relatório de Impacto à Proteção de Dados Pessoais (RIPD)	médio	
39	Planejar medidas de segurança desde a fase de concepção do serviço ou produto que irá tratar dados pessoais (*security by default* e *security by design*)	médio	
40	Elaborar plano de resposta a incidentes relacionados ao tratamento de dados pessoais	médio	
41	Monitorar proativamente a ocorrência de eventos que podem ser associados à violação de dados pessoais	médio	
42	Promover a manutenção de sistemas e serviços que tratam dados pessoais, a fim de adequá-los às normas atinentes ao tema	médio	

Tabela 3. Ações prioritárias a empreender

Assim, de forma orientar o processo, este Programa de Gestão em Privacidade - PGP apresentará o diagnóstico da situação de adequação à Lei Geral de Proteção de Dados Pessoais - LGPD no âmbito da administração central do Ministério da Defesa e organizará as ações a empreender acima relacionadas, em eixos temáticos, conforme apresentado nos tópicos a seguir:

3.1. Diagnóstico da Situação Atual

Dentre as obrigações dos órgãos públicos que exercem as funções típicas de controlador de dados pessoais, algumas são imperativas, para que o tratamento de dados pessoais possa ser realizado, conforme estabelece o art. 23 da Lei Geral de Proteção de Dados Pessoais - LGPD.

> Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:
>
> I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos;
>
> [...]
>
> III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei; [...]

A nomeação do Encarregado pelo Tratamento de Dados Pessoais foi efetuada por meio da Portaria GM-MD nº 1.648, de 9 de abril de 2021, e seus dados de contato foram publicados no site

institucional do Ministério da Defesa, conforme estabelece o § 1º do art. 41 da Lei Geral de Proteção de Dados Pessoais - LGPD.

O art. 50 da Lei Geral de Proteção de Dados Pessoais - LGPD também estabelece que o órgão deve orientar a adoção de boas práticas.

> Art. 50. Os controladores e operadores, no âmbito de suas competências pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.
>
> § 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.
>
> § 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:
>
> I - implementar programa de governança em privacidade que, no mínimo:
>
> a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;
>
> b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;
>
> c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;
>
> d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
>
> e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;
>
> f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;
>
> g) conte com planos de resposta a incidentes e remediação; e
>
> h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;
>
> II - demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei.

> § 3º As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional.

Nesse sentido, o Ministério da Defesa, ao longo do corrente ano, adotou as seguintes medidas, dentre outras:

a) conclusão dos trabalhos do grupo instituído para propor a estrutura e as ações de Proteção de Dados Pessoais;

b) criação do curso de tratamento e proteção de dados pessoais (Portaria nº GM-MD nº 744, de 11 de fevereiro de 2022), cuja primeira turma capacitou 1.630 pessoas que exercem atividade profissional no âmbito do Ministério da Defesa;

c) aprovação da Diretriz para a Proteção de Dados Pessoais (Portaria GM-MD nº 5.814, de 29 de novembro de 2022);

d) promoção de campanhas de conscientização em segurança da informação (*phishing*) relacionando aspectos afetos à proteção de dados pessoais e conscientização com emprego da técnica de gamificação, envolvendo temas de segurança da informação e proteção de dados pessoais.

e) estruturação da governança e gestão: o Comitê de Governança do Ministério da Defesa - CG-MD acompanhará, em nível estratégico, as ações relacionadas ao tratamento de dados pessoais; e a gestão das operações de proteção de dados pessoais será orientada e acompanhada, no âmbito da administração central do Ministério da Defesa, pelo Comitê de Governança Digital do Ministério da Defesa - CGD-MD; e

f) instituição do Núcleo de Segurança da Informação e Privacidade - NUSIP com a finalidade de orientar e acompanhar a gestão da segurança da informação e da proteção de dados pessoais no âmbito da administração central do Ministério da Defesa (Portaria nº GM-MD nº 5.581, de 10 de novembro de 2022).

O resultado destas ações contribui para o incremento do índice de maturidade quanto à adequação à Lei Geral de Proteção de Dados Pessoais - LGPD instituído pelo Ministério da Economia para acompanhar a implementação da Lei Geral de Proteção de Dados Pessoais - LGPD no setor público. A metodologia de mensuração deste índice consiste em responder um autodiagnóstico, por meio de um questionário que congrega as principais orientações da Lei Geral de Proteção de Dados Pessoais - LGPD em sete dimensões, que permite identificar a maturidade do órgão aplicando-se a tabela a seguir:

Nível de Adequação	Resultado do índice
Inicial	0,00 a 0,29
Básico	0,30 a 0,49
Intermediário	0,50 a 0,69
Em aprimoramento	0,70 a 0,89
Aprimorado	0,90 a 1,00

Tabela 4. Nível de adequação à LGPD

Desde 2020, o Ministério da Economia vem demandando aos órgãos públicos a participação neste diagnóstico. O Ministério da Defesa o respondeu em 2020 e em 2021. O Diagnóstico de 2022, até o momento, não foi solicitado oficialmente pelo Ministério da Economia, mas a simulação deste, a partir da ferramenta disponibilizada pelo Ministério da Economia[1], sinaliza que o Ministério da Defesa, com as medidas adotadas, alcançou o nível de maturidade

[1] https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/diagnostico-privacidade-lgpd

intermediário. A tabela a seguir apresenta a evolução da administração central do Ministério da Defesa ao longo dos anos.

Dimensões	2020	2021	2022[2]
Governança	0,24	0,45	0,74
Conformidade Legal e Respeito aos princípios	0,23	0,23	0,42
Transparência e direitos do titular	0,16	0,38	0,64
Rastreabilidade	0,20	0,30	0,30
Adequação de contratos e de relações com parceiros	0,20	0,20	0,50
Segurança da Informação	0,24	0,32	0,38
Violações de dados	0,24	0,55	0,65
Resultado do índice de adequação	**0,22**	**0,35**	**0,52**
Nível de Adequação	**Inicial**	**Básico**	**Intermediário**

Tabela 5. Nível de adequação do MD à LGPD

3.2. Eixos temáticos para implementação das ações a empreender

Eixo Temático 1: Capacitação				
Objetivo	**Meta**	**Prazo**	**Indicador**	**Coordenador**
1.1 Promover a capacitação de pessoas sobre os aspectos gerais da LGPD.	2023: 50% dos usuários de rede capacitados 2024: 100% dos usuários de rede capacitados	2 anos	Índice de conscientização em privacidade	DEADI
Detalhamento				
a) Incluir no plano de desenvolvimento de pessoas a oferta de cursos da trilha de conhecimento 1 do anexo F. (Ação a empreender nº 14)				
b) Incluir o tema proteção de dados pessoais de forma transversal em outras capacitações elaboradas pelo MD.				
c) Fomentar a participação nos cursos incluídos no plano de desenvolvimento de pessoas.				
Objetivo	**Meta**	**Prazo**	**Indicador**	**Coordenador**
1.2 Promover a capacitação específica para as pessoas que tratam dados pessoais com mais frequência.	2023: 50% do efetivo dos setores que tratam dados pessoais com mais frequência capacitados 2024: 100% do efetivo dos setores que tratam dados	2 anos	Índice de conscientização em privacidade	DEADI

[2] O resultado de 2022 foi simulado, não representando informação oficial prestada ao Ministério da Economia.

	pessoais com mais frequência capacitados			
Detalhamento				
a) Incluir no plano de desenvolvimento de pessoas a oferta de cursos da trilha de conhecimento 1 e 2 do anexo F. (Ação a empreender nº 14)				
b) Fomentar a participação nos cursos incluídos no plano de desenvolvimento de pessoas.				
Objetivo	**Meta**	**Prazo**	**Indicador**	**Coordenador**
1.3 Promover a capacitação das pessoas que atuam no setor de recursos humanos, protocolo, transparência e outros que tratam grande volume de dados pessoais.	2023: 50% do efetivo destes setores capacitados 2024: 100% do efetivo destes setores capacitados	2 anos	Índice de conscientização em privacidade	DEADI
Detalhamento				
a) Incluir no plano de desenvolvimento de pessoas a oferta de cursos da trilha de conhecimento 1, 2 e 3 do anexo F. (Ação a empreender nº 14)				
b) Fomentar a participação nos cursos incluídos no plano de desenvolvimento de pessoas				
Objetivo	**Meta**	**Prazo**	**Indicador**	**Coordenador**
1.4 Promover a capacitação daquele que exerce o encargo de Encarregado pelo tratamento de dados pessoais.	2023: realização de 50% dos cursos pelo Encarregado 2024: realização de 100% dos cursos pelo Encarregado	2 anos	Índice de conscientização em privacidade	DEADI
Detalhamento				
a) Incluir no plano de desenvolvimento de pessoas a oferta de cursos da trilha de conhecimento 1, 2, 3, 4, 5 e 6 do anexo F para aquele que estiver designado como Encarregado pelo tratamento de dados pessoais. (Ação a empreender nº 14)				
b) Acompanhar a formação continuada do Encarregado pelo tratamento de dados pessoais.				
Objetivo	**Meta**	**Prazo**	**Indicador**	**Coordenador**
1.5 Promover a capacitação de daqueles que atuam na área de Tecnologia da Informação.	2023: 50% daqueles que atuam na área de TI capacitados 2024: 100% daqueles que atuam na área de TI capacitados	2 anos	Índice de conscientização em privacidade	DEADI
Detalhamento				
a) Incluir no plano de desenvolvimento de pessoas a oferta de cursos da trilha de conhecimento 1, 2, 3, 4 e 5 do anexo F, para aqueles que atuam na área de Tecnologia da Informação. (Ação a empreender nº 14)				
b) Identificar e incluir no plano de desenvolvimento de pessoas a oferta de curso sobre os princípios da privacidade e segurança por padrão e desde a concepção.				
c) Fomentar a participação nos cursos incluídos no plano de desenvolvimento de pessoas				

Eixo Temático 2: Gestão da proteção de dados pessoais no âmbito da administração central do MD				
Objetivo	**Meta**	**Prazo**	**Indicador**	**Coordenador**
2.1 Monitorar a maturidade em proteção de dados pessoais	2023: em aprimoramento 2024: aprimorado	2 anos	Índice de adequação à LGPD	CGD

Detalhamento	**Prazo**	**Responsável**
a) Acompanhar a implementação da estrutura de proteção de dados pessoais, a publicação da Diretriz para a Proteção de Dados Pessoais e a instituição deste PGP. (Ação a empreender nº 01, 02 e 03)	6 meses	CGD
b) Acompanhar a publicação e divulgação de orientações, links documentos relativos ao tema proteção de dados pessoais, preceitos da Diretriz para a Proteção de Dados Pessoais e objetivos e informações sobre o PGP em repositório institucional na intranet. (Ação a empreender nº 04)	2 anos	CGD
c) Acompanhar o plano de comunicação no âmbito do PGP. (Ação a empreender nº 05)	2 anos	CGD
d) Acompanhar indicadores no âmbito PGP. (Ação a empreender nº 06)	2 anos	CGD
e) Apreciar o procedimento para comunicar a Autoridade Nacional de Proteção de Dados e ao titular a ocorrência de incidentes de segurança que possa acarretar risco ou dano relevante aos titulares. (Ação a empreender nº 07)	1 ano	CGD
f) Prever a alocação de recursos para a implementação de mecanismos para tratamento de dados pessoais. (Ação a empreender nº 08)	4 anos	Unidade registra no PDTIC
g) Monitorar a manutenção da designação do Encarregado pelo Tratamento de Dados Pessoais e seus dados de contato no sítio institucional do MD. (Ação a empreender nº 13).	2 anos	CGD

Objetivo	**Meta**	**Prazo**	**Indicador**	**Coordenador**
2.2 Monitorar a publicação de informações sobre o tratamento de dados pessoais no sítio institucional da internet.	2023: sítio institucional 75% atualizado 2024: sítio institucional 100% atualizado	2 anos	Índice de adequação à transparência das operações de tratamento	Encarregado pelo tratamento de dados pessoais

Detalhamento	**Prazo**	**Responsável**
a) Propor a atualização dos dados institucionais sobre proteção de dados pessoais no site da internet, em especial a identificação do encarregado, o canal de atendimento aos direitos dos titulares, a diretriz para a proteção de dados pessoais e os termos de uso e aviso de privacidade dos serviços públicos digitais. (Ação a empreender nº 11)	2 anos	Encarregado pelo tratamento de dados pessoais
b) Implementar sistema de gestão de consentimentos e exercício dos direitos dos titulares. (Ação a empreender nº 12)	4 anos	
c) Avaliar e encaminhar para publicação as hipóteses de tratamento de dados pessoais, informadas pelas unidades finalísticas. (Ação a empreender nº 33)	2 anos	

Eixo Temático 3: Medidas técnicas e administrativas para o tratamento de dados pessoais				
Objetivo	**Meta**	**Prazo**	**Indicador**	**Coordenador**
3.1 Mapear e inventariar os processos que realizam o tratamento de dados pessoais.	2023: 50% das operações de tratamento inventariadas 2024: 100% das operações de tratamento inventariadas	2 anos	Índice de operações de tratamento com dados pessoais inventariados	Encarregado pelo tratamento de dados pessoais

Detalhamento	**Prazo**	**Responsável**
a) Acompanhar a atualização da Política de Segurança da Informação e da Política de classificação da informação. (Ação a empreender nº 15 e 16)	1 ano	Unidade finalística
b) Identificar se o tratamento de dados pessoais é regido por contrato e revisar e adequar contratos e outros instrumentos que prevejam o tratamento de dados pessoais. (Ação a empreender nº 17)	1 ano	Responsáveis por contratos
c) Identificar se existem operadores no tratamento mapeado e regularizar a situação contratual, se necessário. (Ação a empreender nº 18)	1 ano	Responsáveis por contratos
d) Utilizar o modelo de inventário de dados pessoais para registrar os dados mapeados. (Ação a empreender nº 19)	1 ano	Unidade finalística
e) Identificar e documentar os tipos de dados pessoais e dados pessoais sensíveis, as finalidades, as bases legais das atividades de tratamento de dados pessoais no inventário. (Ação a empreender nº 20)	1 ano	Unidade finalística
f) Avaliar se a coleta de dados é a estritamente necessária para a finalidade identificada, caso haja coleta excessiva elaborar um plano de ação para adequar o processo de tratamento de dados pessoais (Ação a empreender nº 21)	1 ano	Unidade finalística
g) Identificar processos de negócio, serviços e sistemas e seus responsáveis que realizam o tratamento de dados pessoais. (Ação a empreender nº 22)	1 ano	Unidade finalística
h) Identificar, a partir dos inventários, as categorias de titulares de dados pessoais com quem o órgão se relaciona. (Ação a empreender nº 23)	1 ano	Unidade finalística
i) Identificar, a partir dos inventários, os dados pessoais que são compartilhados com terceiros. (Ação a empreender nº 25)	1 ano	Unidade finalística
j) Identificar, a partir dos inventários e registrar eventos relacionados à transferência de dados pessoais que são compartilhados com terceiros e a transferência internacional de dados pessoais. (Ação a empreender nº 26 e 27)	1 ano	Unidade finalística
k) Classificar os dados tratados em dados pessoais e dados pessoais sensíveis e avaliar se os dados pessoais são retidos apenas pelo tempo necessário para cumprir a finalidade do tratamento. (Ação a empreender nº 9 e 29)	1 ano	Unidade finalística
l) Revisar e propor a atualização de manuais, normas, instruções e outros instrumentos que prevejam o tratamento de dados pessoais. (Ação a empreender nº 34)	2 anos	Unidade finalística
m) Elaborar Relatório de Impacto à Proteção de Dados Pessoais (RIPD), caso os dados pessoais tratados ensejem riscos às liberdades civis e aos direitos fundamentais dos titulares de dados pessoais. (Ação a empreender nº 37)	2 anos	Unidade finalística

Objetivo	Meta	Prazo	Indicador	Coordenador
3.2 Elaborar e publicar os termos de uso e aviso de privacidade.	2023: 100 % dos serviços públicos digitais da ACMD com termo publicado	6 meses	Índice de termo de uso elaborado	Encarregado pelo tratamento de dados pessoais

Detalhamento	Prazo	Responsável
a) A área responsável pelo serviço público digital deverá elaborar os termos de uso e aviso de privacidade e submeter à aprovação da CONJUR. (Ação a empreender nº 33)	6 meses	Unidade finalística
b) Uma vez aprovados, encaminhar os termos de uso e aviso de privacidade para publicação no sítio institucional do MD na Internet. (Ação a empreender nº 33)	6 meses	Unidade finalística
c) Solicitar a atualização da Carta de Serviços ao usuário para registrar o link do termo de uso e aviso de privacidade. (Ação a empreender nº 33)	6 meses	Unidade finalística

Objetivo	Meta	Prazo	Indicador	Coordenador
3.3 Adequar sistemas e formulários que coletam dados pessoais aos princípios da LGPD e de modo a permitir a rastreabilidade do tratamento do dado pessoal durante todo seu ciclo de vida.	2023: Adequação de 50% sistemas e formulários 2024: Adequação de 100 % sistemas e formulário	2 anos	Índice de adequação de sistemas e formulários que coletam dados pessoais	Encarregado pelo tratamento de dados pessoais

Detalhamento	Prazo	Responsável
a) Elaborar e implementar plano de ação para adequação dos sistemas e formulários. (Diretriz)	2 anos	Unidade finalística
b) Implementar mecanismos para atender os direitos dos titulares de dados pessoais. (Ação a empreender nº 24)	2 anos	Unidade finalística
c) Avaliar os sistemas e formulários que coletam dados pessoais, verificando se a coleta está adequada aos princípios da LGPD. (Ação a empreender nº 28)	2 anos	Unidade finalística
d) Implementar processo formal para registro, cancelamento e provisionamento de usuários em sistemas que realizam o tratamento de dados pessoais. (Ação a empreender nº 35)	4 anos	Unidade finalística
e) Estabelecer medidas para assegurar que processos, serviços ou sistemas sejam projetados, desde a concepção e por padrão, em conformidade com a LGPD (*Privacy by Design* e *Privacy by default*). (Ação a empreender nº 39)	4 anos	Unidade finalística
f) Promover a manutenção de sistemas e serviços que tratam dados pessoais, a fim de adequá-los às normas atinentes ao tema. (Ação a empreender nº 42)	4 anos	Unidade finalística

Eixo Temático 4: Gestão de riscos e prevenção de incidentes				
Objetivo	**Meta**	**Prazo**	**Indicador**	**Coordenador**
4.1 Implementar e acompanhar processo de avaliação de riscos de segurança da informação envolvendo dados pessoais.	2023: 50% das operações de tratamento com risco com RIPD elaborado 2023: 100% das operações de tratamento com risco com RIPD elaborado	2 anos	Índice de operações de tratamento com RIPD elaborado	Unidades finalísticas

Detalhamento	**Prazo**	**Responsável**
a) Planejar medidas de segurança desde a fase de concepção do serviço ou produto que irá tratar dados pessoais (*security by default* e *security by design*). (Ação a empreender nº 10 e 39)	4 anos	Unidade finalística
b) Monitorar vulnerabilidades técnicas nos sistemas e serviços que tratam dados pessoais, a fim de adequá-los às normas atinentes ao tema, a partir dos RIPD elaborados. (Ação a empreender nº 30)	2 anos	Unidade finalística
c) Estabelecer rastreabilidade dos dados pessoais em meio físico e digital e gerar evidências para comprovar que tomou medidas de segurança técnicas e administrativas para proteger os dados pessoais. (Ação a empreender nº 31 e 36)	4 anos	Unidade finalística
d) Realizar gestão de incidentes para tratar possíveis violações dos dados pessoais. (Ação a empreender nº 32)	2 anos	Unidade finalística
e) Implementar controles de segurança para riscos identificados no Relatório de Impacto à Proteção de Dados Pessoais (RIPD). (Ação a empreender nº 38)	2 anos	Unidade finalística
f) Elaborar plano de resposta a incidentes relacionados ao tratamento de dados pessoais. (Ação a empreender nº 40)	4 anos	Unidade finalística
g) Monitorar proativamente a ocorrência de eventos que podem ser associados à violação de dados pessoais. (Ação a empreender nº 41)	4 anos	Unidade finalística

Tabela 6: Eixos temáticos

Para atendimento das ações a empreender previstas nos eixos temáticos, as unidades finalísticas deverão elaborar plano de ação, a partir do mapeamento e inventário de dados pessoais, alinhado com este Programa, para a implementação de processos, procedimentos, controles e demais medidas técnicas e administrativas quanto ao tratamento de dados pessoais.

Assim sendo, a primeira medida a ser adotada por todas as unidades finalísticas é a realização do mapeamento e inventário de dados pessoais. Esta ação é primordial para o processo de adequação à Lei Geral de Proteção de Dados Pessoais - LGPD, visto que o tratamento de dados pessoais não se restringe a um único setor ou área específica. Mediante a realização de um mapeamento de dados e produção do correspondente inventário será possível fazer um balanço das operações de tratamento, verificar se estão em conformidade com os princípios e as bases legais previstas na Lei Geral de Proteção de Dados Pessoais - LGPD e elaborar um plano de ação aderente à realidade das operações de tratamento realizadas pela unidade finalística.

Nos anexos deste Programa de Gestão em Privacidade - PGP são apresentados modelos e orientações para a execução das ações a empreender, visando oportunizar às unidades finalísticas ferramentas para realizar a adequação de seus processos organizacionais à Lei Geral de Proteção de Dados Pessoais - LGPD.

3.3. Monitoramento

Acompanhar a conformidade à Lei Geral de Proteção de Dados Pessoais - LGPD é uma atividade contínua e necessária que precisa ter sustentabilidade ao longo do tempo. Para tanto, deverão ser mensurados e acompanhados indicadores de performance e efetuada a gestão de incidentes envolvendo o tratamento de dados pessoais. Com base nos insumos gerados, poderão ser produzidas análises e reporte de resultados que serão utilizados em prol do processo de melhoria contínua.

Para acompanhar a conformidade à Lei Geral de Proteção de Dados Pessoais - LGPD, o Comitê de Governança Digital - CGD estabelecerá anualmente uma assessoria técnica para relatar a evolução dos indicadores abaixo relacionados:

Indicador	Descrição	Fórmula de Cálculo
Índice de conscientização em privacidade	Acompanhar as ações de capacitação e campanhas de fomento à mentalidade de privacidade. Medição: anual	Quantidade de treinamentos realizados / quantidade de treinamentos ofertados * 100
Índice de adequação à LGPD	Resultados do Diagnóstico de Adequação à LGPD, mensurado com base no modelo proposto pelo Ministério da Economia. Medição: anual	Resultado da aplicação de questionário Linha base: 2020: Inicial 2021: Básico
Índice de adequação à transparência das operações de tratamento	Acompanhar a publicação de informações sobre o tratamento de dados pessoais no sítio institucional da internet.	Total de tipos de informação publicadas / total de tipos de informação de publicação obrigatória * 100
Índice de operações de tratamento com dados pessoais inventariados	Acompanhar o processo de inventário das operações de tratamento de dados pessoais. Medição: anual	Quantidade de operações de tratamento de dados pessoais inventariados
Índice de termo de uso elaborado	Acompanhar o processo de elaboração de termos de uso dos serviços e sistemas externos que realizem o tratamento de dados pessoais. Medição: anual	Quantidade termos de uso elaborados / quantidade de serviços públicos digitais ou sistemas que tratem dados pessoais * 100
Índice de adequação de sistemas e formulários que coletam dados pessoais	Acompanhar a conformidade no que ser refere à coleta de dados pessoais considerando os princípios da LGPD	Quantidade de sistemas e formulários adequados com relação ao total de sistemas e formulários existentes * 100
Índice de operações de tratamento com RIPD elaborado	Acompanhar o processo de elaboração do relatório de impacto dos sistemas	Quantidade de RIPD elaborados / quantidade de operações mapeadas contendo dados pessoais que

Indicador	Descrição	Fórmula de Cálculo
	digitais e dos serviços públicos do MD. Medição: anual	representem risco às liberdades individuais * 100
Incidentes envolvendo dados pessoais	Monitorar e acompanhar o número de incidentes de violação de dados pessoais e/ou vazamento de dados pessoais. Medição: anual	Quantidade de incidentes efetivamente ocorridos / total de incidentes reportados no ano * 100

Tabela 7. Indicadores de performance

4. RESPONSABILIDADES

A Lei Geral de Proteção de Dados Pessoais - LGPD e a Diretriz para a Proteção de Dados Pessoais do Ministério da Defesa estabelecem as seguintes atribuições quanto ao tratamento de dados pessoais.

4.1 Comitê de Governança do Ministério da Defesa (CG-MD):

a) acompanhar, em nível estratégico, as ações relacionadas ao tratamento de dados pessoais, por meio da estrutura de governança estabelecida;

b) apreciar propostas de diretrizes e políticas visando a conformidade com as disposições da Lei nº 13.709, de 2018;

c) promover e acompanhar a implementação de medidas e iniciativas visando o incremento do nível de maturidade quanto à proteção de dados pessoais;

d) fomentar a cultura de privacidade e proteção de dados pessoais; e

e) propor aperfeiçoamentos na estrutura de governança estabelecida para o tratamento de dados pessoais.

4.2 Comitê de Governança Digital do Ministério da Defesa (CGD-MD):

a) orientar e acompanhar a gestão das operações de proteção de dados pessoais no âmbito da administração central do Ministério da Defesa;

b) subsidiar o Comitê de Governança - CG-MD nos temas afetos à proteção de dados pessoais;

c) aprovar este Programa de Gestão em Privacidade -PGP, bem como suas revisões;

d) orientar e monitorar a implementação do Programa de Gestão em Privacidade - PGP, acompanhando seus indicadores; e

e) propor aperfeiçoamentos nas diretrizes, políticas, procedimentos e estruturas relacionados à proteção de dados pessoais.

4.3 Encarregado pelo tratamento de dados pessoais

a) aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

b) receber comunicações da autoridade nacional e adotar providências;

c) orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;

d) apreciar os inventários de dados pessoais e os relatórios de impacto à proteção de dados pessoais e orientar as unidades organizacionais quanto aos riscos identificados;

e) providenciar a divulgação no sítio institucional da intranet, na área proteção de dados pessoais, informações e o canal oficial interno para registro de requisições e ocorrências envolvendo o tratamento de dados pessoais; e

f) encaminhar à Assessoria Especial de Comunicação Social do Ministério da Defesa, sempre que houver atualização, as informações para a divulgação, no sítio eletrônico institucional, a respeito dos procedimentos de tratamento de dados.

4.4 Gestor de Segurança da Informação

a) dar ciência do incidente ao Ministro de Estado de Defesa;

b) coordenar as medidas técnicas e administrativas para cessar o incidente;

c) elaborar comunicado de incidente dirigido à Autoridade Nacional de Proteção de Dados - ANPD e aos respectivos titulares, observados os prazos estabelecidos e procedimentos adotados pela Autoridade Nacional de Proteção de Dados - ANPD;

d) acompanhar as medidas afetas ao incidente até o término de seus efeitos;

e) apreciar os relatórios de vulnerabilidades e as propostas de tratamento dos riscos apresentados pelas unidades organizacionais e orientá-las quanto às adequações necessárias e compatíveis;

f) apreciar os inventários de dados pessoais e os relatórios de impacto à proteção de dados pessoais e orientar as unidades organizacionais quanto aos riscos identificados; e

g) apreciar os riscos identificados nos sistemas e bancos de dados em que houver o tratamento de dados pessoais e prestar as orientações necessárias.

4.5 Núcleo de Segurança da Informação e Privacidade - NUSIP

a) propor a organização dos processos, estruturas, diretrizes e procedimentos com vistas ao aperfeiçoamento da gestão da segurança da informação e da proteção de dados pessoais;

b) orientar e acompanhar a implementação e o desenvolvimento da gestão da segurança da informação e da proteção de dados pessoais;

c) disseminar informações sobre leis, normativos ou padrões e propor iniciativas visando o incremento do nível de maturidade ou o fortalecimento da cultura quanto à segurança da informação e à proteção de dados pessoais; e

d) subsidiar o Comitê de Governança do Ministério da Defesa - CG-MD (Portaria GM-MD nº 3.127/2021), o Comitê de Governança Digital do Ministério da Defesa - CGD-MD (Portaria GM-MD nº 3.572/2022) e o Comitê de Segurança da Informação (Portaria GM-MD nº 3.247/2022).

4.6 Unidades organizacionais responsáveis pelo tratamento de dados pessoais

a) informar ao Gestor de Segurança da Informação os assuntos afetos à gestão de incidentes e vulnerabilidades no âmbito do tratamento de dados pessoais;

b) mapear as atividades de tratamento e realizar o inventário dos dados pessoais tratados, mantendo-o atualizado;

c) garantir que o inventário de dados pessoais contenha os registros e fluxos de tratamento dos dados, com base na consolidação do mapeamento dos serviços e processos de negócio que realizem o tratamento de dados pessoais;

d) elaborar plano de ação, alinhado com o Programa de Gestão em Privacidade -PGP, para aperfeiçoar as operações de tratamento de dados pessoais mapeadas;

e) identificar lacunas à proteção de dados pessoais nos processos geridos, avaliar os riscos decorrentes e elaborar, sempre que necessário, o relatório de impacto à proteção de dados pessoais (RIPD);

f) apresentar ao Gestor de Segurança da Informação a minuta do Relatório de Impacto à Proteção de Dados Pessoais - RIPD com a proposta para tratamento dos riscos e implementar as adequações necessárias e compatíveis conforme orientação daquele Gestor;

g) encaminhar cópia atualizada do inventário de dados pessoais e do RIPD ao Gestor de Segurança da Informação e ao Encarregado pelo Tratamento de Dados Pessoais;

h) arquivar o inventário de dados pessoais e os relatórios de impacto à proteção de dados pessoais, permanecendo em condições de disponibilizá-los, em caso de solicitação da Autoridade Nacional de Proteção de Dados - ANPD ou de outro órgão de controle;

i) elaborar o relatório de impacto à proteção de dados pessoais quando necessário;

j) adotar medidas de transparência aos usuários sobre o tratamento de dados pessoais, por meio do sítio institucional do Ministério da Defesa da internet;

k) fazer cumprir, no âmbito de suas atribuições e competências, a Política de Segurança da Informação;

l) determinar, no âmbito de suas atribuições e competências, que terceiros contratados estejam em conformidade com a Lei Geral de Proteção de Dados Pessoais - LGPD;

m) incentivar a participação em eventos de capacitação, visando estimular a cultura de proteção de dados pessoais;

n) implementar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais, ou não, de eliminação, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito;

o) monitorar preventivamente os eventos relacionados no relatório de impacto à proteção de dados pessoais, visando evitar incidentes envolvendo dados pessoais;

p) prestar todas as informações e adotar as medidas necessárias para apurar a natureza dos dados pessoais afetados;

q) informar quais os titulares de dados pessoais foram atingidos pelo incidente;

r) indicar as medidas técnicas e de segurança utilizadas para a proteção dos dados e as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo decorrente do incidente, empregando, sempre que possível, plano de resposta a incidentes; e

s) revisar e adequar todos os contratos que envolvam as atividades de tratamento de dados pessoais às normas de privacidade e proteção de dados pessoais, considerando a responsabilização dos agentes de tratamento

6. REVISÃO

Este programa deverá ser revisado a cada dois anos ou sempre que determinado pelo Comitê de Governança Digital.

7. REFERÊNCIAS

- Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais;

- Decreto nº 8.638, de 15 de janeiro de 2016, instituiu a Política de Governança Digital;

- Decreto nº 9.759, de 11 de abril de 2019, extingue e estabelece diretrizes, regras e limitações para colegiados da administração pública federal;

- Decreto nº 10.046, de 9 de outubro de 2019, dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados;

- Decreto nº 10.332, de 29 de abril de 2020, aprovou a Estratégia de Governo Digital (2020 a 2022);

- Guia de Boas Práticas da LGPD, disponível no link: https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaLGPD.pdf;

- Guia de elaboração de Programa de Governança em Privacidade, disponível no link: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_governanca_privacidade.pdf;

- Guia Orientativo para definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado, disponível no link: https://www.gov.br/anpd/pt-br/assuntos/noticias/2021-05-27-guia-agentes-de-tratamento_final.pdf;

- Guia de Tratamento de dados pessoais pelo setor público, disponível no link: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf; e

- Instrução normativa SGD/ME Nº 117, de 19 de novembro de 2020, dispõe sobre a indicação do Encarregado pelo Tratamento dos Dados Pessoais no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional.

8. ANEXOS

Anexo A - Modelo de inventário de dados pessoais;

Anexo B - Modelo de Relatório de impacto à proteção de dados pessoais (RIPD);

Anexo C - Modelo de Aviso de Privacidade e Termo de uso;

Anexo D - Procedimentos em caso de incidentes envolvendo dados pessoais;

Anexo E - Plano de comunicação relativo ao tratamento de dados pessoais; e

Anexo F - Trilhas de conhecimento na área de proteção de dados pessoais.

9. APROVAÇÃO

Este Programa de Gestão em Privacidade foi apreciado pelo Comitê de Governança Digital do Ministério da Defesa - CGD-MD, conforme deliberação de 29 de março de 2023, assentada na Ata da Reunião nº 136.

ANEXO A
MODELO DE INVENTÁRIO DE DADOS PESSOAIS

Inventário de Dados Pessoais

Essa guia é um modelo de um formulário operacional a ser reproduzido e preenchido de acordo com a sua atividade de tratamento de dados pessoais. São fornecidos comentários adicionais como notas para auxiliar no preenchimento do formulário (Nota em vermelho na célula).

1 - Identificação dos serviços / processo de negócio de tratamento de dados pessoais					
1.1 - Nome do serviço / Processo de negócio					
1.2 - Nº Referência / ID		**Secretaria/Departamento/Coordenação:**			
1.3 - Data de Criação do Inventário					
1.4 - Data Atualização do Inventário					
2 - Agentes de Tratamento e Encarregado	**Nome**	**Endereço**	**CEP**	**Telefone**	**E-mail**
2.1 - Controlador	Ministério da Defesa (MD)	Esplanada dos Ministérios, Bloco Q	70.049-900	(61) 3312-4000	sic@defesa.gov.br
2.2 - Encarregado		Esplanada dos Ministérios, Anexo I, Bloco Q	70.049-900		encarregado@defesa.gov.br
2.3 - Operador					
3 - Fases do Ciclo de Vida do Tratamento Dados Pessoais	**Coleta**	**Retenção**	**Processamento**	**Compartilhamento**	**Eliminação**

3.1 - Em qual fase do ciclo de vida o Operador atua					
4 - De que forma (como) os dados pessoais são coletados, retidos/armazenados, processados/usados, compartilhados e eliminados					
4.1 - Descrição do Fluxo do tratamento dos dados pessoais					
5 - Escopo e Natureza dos Dados Pessoais					
5.1 - Abrangência da área geográfica do tratamento					
5.2 - Fonte de dados utilizada para obtenção dos dados pessoais					
6 - Finalidade do Tratamento de Dados Pessoais					
6.1 - Hipótese de Tratamento					
6.2 - Finalidade					
6.3 - Previsão legal					
6.4 - Resultados pretendidos para o titular de dados					
6.5 - Benefícios esperados para o órgão, entidade ou para a sociedade como um todo					
7 - Categoria de Dados Pessoais					
7.1 -Dados de Identificação Pessoal	**Descrição**	**Tempo Retenção dos Dados**	**Fonte Retenção**	**Nome Base de Dados**	
7.1.1 - Informações de identificação pessoal					
7.1.2 - Informações de identificação atribuídas por instituições governamentais					

7.1.3 - Dados de identificação eletrônica				
7.1.4 - Dados de localização eletrônica				
7.2 -Dados Financeiros	**Descrição**	**Tempo Retenção dos Dados**	**Fonte Retenção**	**Nome Base de Dados**
7.2.1 - Dados de identificação financeira				
7.2.2 - Recursos financeiros				
7.2.3 - Dívidas e despesas				
7.2.4 - Situação financeira (Solvência)				
7.2.5 - Empréstimos, hipotecas, linhas de crédito				
7.2.6 - Assistência financeira				
7.2.7 - Detalhes da apólice de seguro				
7.2.8 - Detalhes do plano de pensão				
7.2.9 - Transações financeiras				
7.2.10 - Compensação				
7.2.11 - Atividades profissionais				
7.2.12 - Acordos e ajustes				
7.2.13 - Autorizações ou consentimentos				
7.3 - Características Pessoais	**Descrição**	**Tempo Retenção dos Dados**	**Fonte Retenção**	**Nome Base de Dados**
7.3.1 - Detalhes pessoais				
7.3.2 - Detalhes militares				
7.3.3 - Situação de Imigração				

7.3.4 - Descrição Física				
7.4 - Hábitos Pessoais	**Descrição**	**Tempo Retenção dos Dados**	**Fonte Retenção**	**Nome Base de Dados**
7.4.1 - Hábitos				
7.4.2 - Estilo de vida				
7.4.3 - Viagens e deslocamentos				
7.4.4 - Contatos sociais				
7.4.5 - Posses				
7.4.6 - Denúncias, incidentes ou acidentes				
7.4.7 - Distinções				
7.4.8 - Uso de mídia				
7.5 - Características Psicológicas	**Descrição**	**Tempo Retenção dos Dados**	**Fonte Retenção**	**Nome Base de Dados**
7.5.1 - Descrição Psicológica				
7.6 - Composição Familiar	**Descrição**	**Tempo Retenção dos Dados**	**Fonte Retenção**	**Nome Base de Dados**
7.6.1 - Casamento ou forma atual de coabitação				
7.6.2 - Histórico conjugal				
7.6.3 - Familiares ou membros da família				
7.7 - Interesses de lazer	**Descrição**	**Tempo Retenção dos Dados**	**Fonte Retenção**	**Nome Base de Dados**
7.7.1 - Atividades e interesses de lazer				

7.8 - Associações	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.8.1 Associações (exceto profissionais, políticas, em sindicatos ou qualquer outra associação que se enquadre em dados pessoais sensíveis)				
7.9 - Processo Judicial/Administrativo/Criminal	**Descrição**	**Tempo Retenção dos Dados**	**Fonte Retenção**	**Nome Base de Dados**
7.9.1 - Suspeitas				
7.9.2 - Condenações e sentenças				
7.9.3 - Ações judiciais				
7.9.4 - Penalidades Administrativas				
7.10 - Hábitos de Consumo	**Descrição**	**Tempo Retenção dos Dados**	**Fonte Retenção**	**Nome Base de Dados**
7.10.1 - Dados de bens e serviços				
7.11 - Dados Residenciais	**Descrição**	**Tempo Retenção dos Dados**	**Fonte Retenção**	**Nome Base de Dados**
7.11.1 - Residência				
7.12 - Educação e Treinamento	**Descrição**	**Tempo Retenção dos Dados**	**Fonte Retenção**	**Nome Base de Dados**
7.12.1 - Dados acadêmicos/escolares				
7.12.2 Registros financeiros do curso/treinamento				
7.12.3 - Qualificação e experiência profissional				
7.13 - Profissão e emprego	**Descrição**	**Tempo Retenção dos Dados**	**Fonte Retenção**	**Nome Base de Dados**

7.13.1 - Emprego atual				
7.13.2 - Recrutamento				
7.13.3 - Rescisão de trabalho				
7.13.4 - Carreira				
7.13.5 - Absentismo e disciplina				
7.13.6 -Avaliação de Desempenho				
7.14 -Registros/gravações de vídeo, imagem e voz	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.14.1 - Vídeo e imagem				
7.14.2 - Imagem de Vigilância				
7.14.3 - Voz				
7.15 -Outros (Especificar)	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.15.1 - Outros (Especificar)				
8 - Categorias de Dados Pessoais Sensíveis	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
8.1 - Dados que revelam origem racial ou ética				
8.2 - Dados que revelam convicção religiosa				
8.3 - Dados que revelam opinião política				
8.4 - Dados que revelam filiação a sindicato				
8.5 - Dados que revelam filiação a organização de caráter religioso				

8.6 - Dados que revelam filiação ou crença filosófica				
8.7 - Dados que revelam filiação ou preferências política				
8.8 - Dados referentes à saúde ou à vida sexual				
8.9 - Dados genéticos				
8.10 - Dados biométricos				
9 - Frequência e totalização das categorias de dados pessoais tratados				
9.1 - Frequência de tratamento dos dados pessoais				
9.2 - Quantidade de dados pessoais e dados pessoais sensíveis tratados				
10 - Categorias dos titulares de dados pessoais	**Tipo de Categoria**	**Descrição**		
10.1 - Categoria 1				
10.2 - Categoria 2				
10.3 - Trata dados de crianças e adolescentes				
10.4 - Além de crianças e adolescente trata dados de outro grupo vulnerável				
11 - Compartilhamento de Dados Pessoais	**Dados pessoais compartilhados**	**Finalidade do compartilhamento**		
11.1 - Nome da Instituição 1				
11.2 - Nome da Instituição 2				
11.3 - Nome da Instituição 3				
11.4 - Nome da Instituição 4				

12 - Medidas de Segurança/Privacidade	Tipo de medida de segurança e privacidade		Descrição do(s) Controle(s)
12.3 - Medida de Segurança/Privacidade 1			
12.2 - Medida de Segurança/Privacidade 2			
12.3 - Medida de Segurança/Privacidade 3			
13 - Transferência Internacional de Dados Pessoais	**País**	**Dados pessoais transferidos**	**Tipo de garantia para transferência**
13.1 - Organização 1			
13.2 - Organização 2			
13.3 - Organização 3			
14 - Contrato(s) de serviços e/ou soluções de TI que trata(m) dados pessoais do serviço/processo de negócio	**Nº Processo Contratação**	**Objeto do Contrato**	**E-mail do Gestor do Contrato**
14.2 - Contrato nº 1			
14.2 - Contrato nº 2			

ANEXO B
MODELO DE RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

MINISTÉRIO DA
DEFESA

<Secretaria - Geral>

<Estado-Maior Conjunto das Forças Armadas>

<Secretaria ...>

RELATÓRIO DE IMPACTO
À PROTEÇÃO DE DADOS PESSOAIS

Brasília

<nº>ª edição – 202X

MINISTRO DE ESTADO DA DEFESA - MD -
CHEFE DO ESTADO-MAIOR CONJUNTO DAS FORÇAS ARMADAS – EMCFA -
SECRETÁRIO GERAL - SG -
SECRETÁRIO DE ... -
DEPARTAMENTO DE ... -

EQUIPE DE ELABORAÇÃO DO RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS (RIPD)	
Coordenação do RIPD/MD	<nome do coordenador>
Representantes	<nome dos representantes das áreas envolvidas neste relatório>

ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS
- <nome do Encarregado>

ATENÇÃO!

<Os trechos marcados em azul neste devem ser editados, substituídos ou excluídos, conforme necessário>.

Sumário

HISTÓRICO DE REVISÕES

DATA	VERSÃO	DESCRIÇÃO	AUTOR
xx/xx/202x	1.0	Conclusão da primeira versão do relatório	xxx

LISTA DE TABELAS

ABREVIATURAS, SIGLAS E ACRÔNIMOS

1. Tabela de Abreviaturas, Siglas e Acrônimos

4. OBJETIVO

O Relatório de Impacto à Proteção de Dados Pessoais - RIPD visa descrever os processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

Este Relatório de Impacto à Proteção de Dados Pessoais - RIPD abrange a operação de tratamento de dados pessoais denominada <nome da operação de tratamento> realizada pelo <departamento> da <Secretaria>.

Referência: art. 5º, XVII da Lei 13.709, de 14 de agosto de 2018 (LGPD).

5. IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO

Controlador
Ministério da Defesa

Encarregado	
<nome do encarregado>	
E-mail do Encarregado	**Telefone do Encarregado**
encarregado@defesa.gov.br	**<telefone do encarregado>**

Operadores
Empresas ou Instituições extra Ministério da Defesa que contratadas ou conveniadas para tratar dados pessoais em nome desta Pasta.

6. NECESSIDADE DE ELABORAR O RELATÓRIO

<Os casos específicos previstos pela Lei Geral de Proteção de Dados Pessoais - LGPD em que o Relatório de Impacto à Proteção de Dados Pessoais - RIPD deverá ou poderá ser solicitado são:

• 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 Lei Geral de Proteção de Dados Pessoais - LGPD em decorrência do tratamento de dados pessoais por órgãos públicos (arts. 31 e 32 combinados); e

• a qualquer momento sob determinação da Autoridade Nacional de Proteção de Dados - ANPD (art. 38).>

<Além dos casos específicos previstos pela Lei Geral de Proteção de Dados Pessoais - LGPD é indicada a elaboração ou atualização do Relatório de Impacto à Proteção de Dados Pessoais

- RIPD 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>.

<Quando for necessária a elaboração do RIPD, 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 Relatório de Impacto à Proteção de Dados Pessoais - RIPD para todas as operações de tratamento de dados pessoais ou de um Relatório de Impacto à Proteção de Dados Pessoais - RIPD para cada projeto, sistema, ou serviço deve ser considerada de acordo com os processos internos de trabalho. Assim, quem realiza o tratamento de quantidade reduzida de dados pessoais, com poucos processos e serviços, pode optar por um Relatório de Impacto à Proteção de Dados Pessoais - RIPD único. Já quem 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 Relatório de Impacto à Proteção de Dados Pessoais - RIPD não seja a opção mais indicada, optando por elaborar Relatórios de Impacto à Proteção de Dados Pessoais - RIPDs segregados por ser mais adequado à sua realidade>.

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

7. 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>.

<A Lei Geral de Proteção de Dados Pessoais - 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>.

7.1. Natureza do Tratamento

<A natureza representa como 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 são compartilhados e quais são esses dados;

• 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, em especial o inventário de dados pessoais>.

7.2. Escopo do Tratamento

<O **escopo** representa a abrangência do tratamento de dados>.

< Nesse sentido, considerar destacar:

• as informações sobre os tipos dos dados pessoais tratados, ressaltando quais dos dados 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>.

7.3. Contexto do Tratamento

<Nesta seção, 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 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;

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

7.4. 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 seção, é importante detalhar o que se pretende alcançar com o tratamento dos dados pessoais, em harmonia com as hipóteses elencadas abaixo arts. 7 º e 11 da Lei Geral de Proteção de Dados Pessoais - LGPD, no que for aplicável>

<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.

• Informar os benefícios esperados para o MD ou para a sociedade como um todo>.

<Recomenda-se ler o guia orientativo para tratamento de dados pessoais no Poder Público disponível em https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf para compreender sobre o estabelecimento das bases legais que amparam o tratamento de dados pessoais e seu emprego no Poder Público>.

8. 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>.

<Nessa seção, 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 de 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>.

9. NECESSIDADE E PROPORCIONALIDADE

<Descrever como se 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:

I - A fundamentação legal para o tratamento dos dados pessoais.

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

a) esse tratamento de dados pessoais é indispensável;

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

c) esse processamento de fato auxilia no propósito almejado.

III - Como será garantida a qualidade [exatidão, clareza, relevância e atualização dos dados] e minimização dos dados.

IV - Quais medidas são adotadas a fim de assegurar que o operador (LGPD, art. 5º, VII) realize o tratamento de dados pessoais conforme a Lei Geral de Proteção de Dados Pessoais - LGPD e respeite os critérios estabelecidos pela instituição que exerce o papel de controlador (LGPD, art. 5º, VI).

V - Como estão implementadas as medidas que asseguram o direito do titular dos dados pessoais obter do controlador o previsto pelo art. 18 da Lei Geral de Proteção de Dados Pessoais - LGPD.

VI - Como a instituição pretende fornecer informações de privacidade para os titulares dos dados pessoais.

VII - Quais são as salvaguardas para as transferências internacionais de dados>

< O artigo 18 da Lei Geral de Proteção de Dados Pessoais - 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>.

10. IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

<O art. 5º, XVII da Lei Geral de Proteção de Dados Pessoais - 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>.

<Como exemplo, 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>.

Os parâmetros escalares adotados neste documento são apresentados na tabela a seguir:

Classificação	Valor
Baixo	5
Moderado	10
Alto	**15**

A figura a seguir apresenta a Matriz Probabilidade X Impacto, instrumento de apoio para a definição dos critérios de classificação do nível de risco.

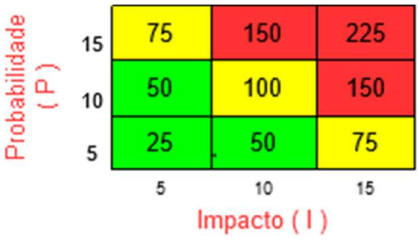

Figura 1: Matriz Probabilidade X Impacto

<O produto da probabilidade pelo impacto de cada risco deve se enquadrar em uma região da matriz apresentada pela Figura 1.

Risco enquadrado na região:

a) verde, é entendido como baixo;

b) amarelo, representa risco moderado; e

c) vermelho, indica risco alto>.

<As definições e conceitos de riscos adotados neste documento são utilizados como forma de ilustrar a identificação e avaliação de riscos realizada no Relatório de Impacto à Proteção de Dados Pessoais - RIPD. Desse modo, é 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 Ministério da Defesa, caso instituída, conforme preconizado pela **Instrução Normativa Conjunta MP/CGU nº 1, de 10 de maio de 2016**>.

ID	RISCO REFERENTE AO TRATAMENTO DE DADOS PESSOAIS	P[3]	I[4]	NÍVEL DE RISCO (P X I)[5]
R01	<Risco 1>			
R02	<Risco 2>			
R03	<Risco N>			

Legenda: P - Probabilidade; I - Impacto.

<A título de informação, é destacada a seguir uma lista não exaustiva de riscos de privacidade e de segurança da informação relacionados com a proteção de dados pessoais. **O nível de probabilidade, impacto e nível de riscos indicados são apenas exemplificativos, devendo ser avaliados de acordo com o contexto do tratamento de dados pessoais**. Os doze primeiros riscos representam riscos de privacidade obtidos da norma ISO/IEC 29134:2017 seção 6.4.4>.

ID	RISCO REFERENTE AO TRATAMENTO DE DADOS PESSOAIS	P	I	Nível de Risco (P x I)
R01	Acesso não autorizado.	10	15	150
R02	Modificação não autorizada.	10	15	150
R03	Perda.	5	15	75
R04	Roubo.	5	15	75
R05	Remoção não autorizada.	5	15	75
R06	Coleção excessiva.	10	10	100
R07	Informação insuficiente sobre a finalidade do tratamento.	10	15	150
R08	Tratamento sem consentimento do titular dos dados pessoais (Caso o tratamento não esteja previsto em legislação ou regulação pertinente).	10	15	150
R09	Falha em considerar os direitos do titular dos dados pessoais (Ex.: perda do direito de acesso).	5	15	75
R10	Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular dos dados pessoais.	10	15	150
R11	Retenção prolongada de dados pessoais sem necessidade.	10	5	50
R12	Vinculação/associação indevida, direta ou indireta, dos dados pessoais ao titular.	5	15	75

[3] Probabilidade: chance de algo acontecer, não importando se definida, medida ou determinada objetiva ou subjetivamente, qualitativa ou quantitativamente; ou se descrita utilizando-se termos gerais ou matemáticos (ISO/IEC 31000:2009, item 2.19).

[4] Impacto: resultado de um evento que afeta os objetivos (ISO/IEC 31000:2009, item 2.18).

[5] Nível de Risco: magnitude de um risco ou combinação de riscos, expressa em termos da combinação das consequências e de suas probabilidades (ISO/IEC 31000:2009, item 2.23 e IN SGD/ME nº 1, de 2019, art. 2º, inciso XIII).

R13	Falha/erro de processamento (Ex.: execução de script de banco de dados que atualiza dado pessoal com dado equivocado, ausência de validação dos dados de entrada, etc.).	5	15	75
R14	Reidentificação de dados pseudonimizados.	5	15	75

11. 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 coluna "Medida(s)" pode ser preenchida com uma medida de segurança ou controle específico adotado para tratamento do risco identificado na seção 7 deste Relatório>.

<Nem sempre é preciso 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 as dificuldades de mitigação. **No entanto, se houver um risco residual de nível alto, é recomendável consultar a Autoridade Nacional de Proteção de Dados - ANPD antes de prosseguir com as operações de tratamento dos dados pessoais**>.

RISCO	MEDIDA(S)	EFEITO SOBRE RISCO[6]	RISCO RESIDUAL[7]			MEDIDA(S) APROVADA(S)[8]
			P	I	(P X I)	
<Risco 1>	<Medida 1; Medida 2; Medida N>					
<Risco 2>	<Medida 1; Medida 2; Medida N>					
<Risco N>	<Medida 1; Medida 2; Medida N>					

Legenda: P – Probabilidade; I – Impacto.

<A seguir são apresentados exemplos de medidas para tratar os riscos a fim de demonstrar o preenchimento da tabela anterior>.

[6] Efeito resultante do tratamento do risco com a aplicação da(s) medida(s) descrita(s) na tabela. As seguintes opções podem ser selecionadas: Reduzir, Evitar, Compartilhar e Aceitar.

[7] Risco residual é o risco que ainda permanece mesmo após a aplicação de medidas para tratá-lo.

[8] Medida aprovada pelo controlador dos dados pessoais. Preencher a coluna com: Sim ou Não.

RISCO	MEDIDA(S)	EFEITO SOBRE RISCO[9]	RISCO RESIDUAL[10]			MEDIDA(S) APROVADA(S)[11]
			P	I	(P X I)	
R01 Acesso não autorizado.	1. Controle de acesso lógico 2. Desenvolvimento seguro 3. Segurança em redes	Reduzir	5	10	50	Sim
R04 Roubo.	1. Controle de acesso lógico 2.Controles criptográficos 3. Proteção física e do ambiente	Reduzir	5	5	25	Sim
R06 Coleção excessiva.	1. Limitação da coleta.	Reduzir	5	10	50	Sim

10. APROVAÇÃO

<Esta seção **visa formalizar a aprovação do Relatório de Impacto à Proteção de Dados Pessoais - RIPD** por meio da obtenção das assinaturas dos Responsáveis pela elaboração do Relatório de Impacto à Proteção de Dados Pessoais - RIPD, pelo encarregado e pelas autoridades que representam o controlador e operador, se for o caso>.

<**O Relatório de Impacto à Proteção de Dados Pessoais - RIPD deve ser revisto e atualizado anualmente ou sempre que existir qualquer tipo de mudança que afete o tratamento dos dados pessoais** realizados. Detalhes sobre a necessidade de revisão do Relatório de Impacto à Proteção de Dados Pessoais - RIP) podem ser observados no **item 2.5.2.9 do Guia de Boas Práticas Lei Geral de Proteção de Dados Pessoais - LGPD, disponível em**: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-lgpd.pdf>

<Local>, <dia> de <mês> de <ano>

COORDENADOR DA EQUIPE DE ELABORAÇÃO DO RELATÓRIO DE IMPACTO	ENCARREGADO
_____ <Nome do responsável> **Matrícula/SIAPE:** xxxxx	_____ <Nome do encarregado> **Matrícula/SIAPE:** xxxxx

AUTORIDADE REPRESENTANTE	AUTORIDADE REPRESENTANTE

[9] Efeito resultante do tratamento do risco com a aplicação da(s) medida(s) descrita(s) na tabela. As seguintes opções podem ser selecionadas: Reduzir, Evitar, Compartilhar e Aceitar.

[10] Risco residual é o risco que ainda permanece mesmo após a aplicação de medidas para tratá-lo.

[11] Medida aprovada pelo controlador dos dados pessoais. Preencher a coluna com: Sim ou Não.

DO CONTROLADOR (NÍVEL SECRETARIA)	DO OPERADOR (SE FOR O CASO)
_____ <Nome do representante> **Matrícula/SIAPE:** xxxxx	_____ <Nome do representante> **Matrícula/SIAPE:** xxxxx

MINISTÉRIO DA DEFESA	**MINISTÉRIO DA DEFESA** **PROGRAMA DE GESTÃO EM PRIVACIDADE**
ANEXO C **MODELO DE TERMO DE USO E AVISO DE PRIVACIDADE**	

Nome do Serviço Público Digital ou Sistema

TERMOS DE USO

1. Aceitação dos Termos de Uso

O uso do serviço está condicionado à aceitação deste Termo e das políticas a ele associadas, devendo o usuário ler e compreender previamente todas as suas cláusulas e condições.

Ao utilizar o serviço, o usuário manifesta sua livre, expressa e inequívoca concordância com relação ao conteúdo deste Termo de Uso e estará legalmente vinculado a todas as condições e compromissos aqui previstos.

2. Definições

Para melhor compreensão deste documento, recomenda-se consultar as definições constantes do artigo 5º da Lei nº 13.709 de 14 de agosto de 2018 e do Glossário de Segurança da Informação.

Além disto, para fins deste Termo de Uso, são aplicáveis as seguintes definições:

- Listar as definições utilizadas neste documento e relevantes para o entendimento do serviço público digital ou sistema

3. Arcabouço Legal

a) Lei nº 12.527, de 18 de novembro de 2011: Lei de Acesso à Informação - Regula o acesso a informações previsto na Constituição Federal.

b) Decreto nº 7.724, de 16 de maio de 2012: Regulamenta a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), que dispõe sobre o acesso a informações previsto na Constituição.

c) Lei nº 12.965, de 23 de abril de 2014: Marco Civil da Internet - Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

d) Lei nº 13.709, de 14 de agosto de 2018: Lei Geral de Proteção de Dados Pessoais - LGPD.

e) Portaria GSI/PR nº 93, de 26 de setembro de 2019: Aprova o Glossário de Segurança da Informação.

- Listar a legislação específica sobre o serviço público digital ou sistema.

4. Descrição do serviço

O “nome do serviço público digital ou sistema” tem como principais finalidades: relacionar a finalidade.

- Inserir o Nome do Serviço.
- Inserir o(a) Nome da Instituição responsável pelo serviço.
- Inserir neste campo, de forma explicativa, a descrição do serviço.

- Trazer tópicos relacionados ao seu objetivo, função, finalidade e outras informações importantes para esclarecer do que trata o serviço prestado.

5. Direitos do usuário do serviço

De acordo com a Lei nº 13.460, de 26 de junho de 2017, são direitos básicos do usuário:

I - Participação no acompanhamento da prestação e na avaliação dos serviços;

II - Obtenção e utilização dos serviços com liberdade de escolha entre os meios oferecidos e sem discriminação;

III - Acesso e obtenção de informações relativas à sua pessoa constantes de registros ou bancos de dados, observado o disposto no inciso X do **caput** do art. 5º da Constituição Federal e na Lei nº 12.527, de 18 de novembro de 2011;

IV - Proteção de suas informações pessoais, nos termos da Lei nº 12.527, de 18 de novembro de 2011;

V - Atuação integrada e sistêmica na expedição de atestados, certidões e documentos comprobatórios de regularidade; e

VI - Obtenção de informações precisas e de fácil acesso nos locais de prestação do serviço, assim como sua disponibilização na internet, especialmente sobre:

a) horário de funcionamento das unidades administrativas;

b) serviços prestados pelo órgão ou entidade, sua localização exata e a indicação do setor responsável pelo atendimento ao público;

c) acesso ao agente público ou ao órgão encarregado de receber manifestações;

d) situação da tramitação dos processos administrativos em que figure como interessado; e

e) valor das taxas e tarifas cobradas pela prestação dos serviços, contendo informações para a compreensão exata da extensão do serviço prestado.

6. Responsabilidade do usuário

O usuário se responsabiliza pela precisão e veracidade dos dados informados e reconhece, que a inconsistência dos mesmos, poderá comprometer a utilização do serviço público digital ou sistema.

Durante a utilização do sistema, a fim de resguardar e de proteger os direitos de terceiros, o usuário se compromete a fornecer somente seus dados pessoais, e os de terceiros para os quais seja o representante legal.

O **login** e senha no serviço público digital ou sistema só poderão ser utilizados pelo usuário cadastrado. Ele se compromete em manter o sigilo da senha, que é pessoal e intransferível, não sendo possível, em qualquer hipótese, a alegação de uso indevido, caso os compartilhe.

O usuário do serviço público digital ou sistema é responsável pela atualização das suas informações pessoais e consequências na omissão ou erros nas informações pessoais cadastradas.

O Usuário é responsável pela reparação de todos e quaisquer danos, diretos ou indiretos (inclusive decorrentes de violação de quaisquer direitos de outros usuários, de terceiros, inclusive direitos de propriedade intelectual, de sigilo e de personalidade), que sejam causados à

Administração Pública, a qualquer outro Usuário, ou, ainda, a qualquer terceiro, inclusive em virtude do descumprimento do disposto nestes Termos de Uso e Aviso de Privacidade ou de qualquer ato praticado a partir do acesso a este serviço público digital ou sistema.

7. Responsabilidades ao acessar ao serviço

O Ministério da Defesa não poderá ser responsabilizado pelos seguintes fatos:

I - Equipamento infectado ou invadido por atacantes;

II - Equipamento avariado no momento da utilização do serviço público digital ou sistema;

III - Proteção do computador;

IV - Proteção das informações baseadas nos computadores dos usuários;

V - Abuso de uso dos computadores dos usuários;

VI - Monitoração clandestina do computador dos usuários;

VII - Vulnerabilidades ou instabilidades existentes nos sistemas dos usuários;

VIII - Perímetro inseguro;

Em nenhuma hipótese, a Administração Pública Federal será responsável pela instalação no equipamento do Usuário ou de terceiros, de códigos maliciosos (vírus, **trojans, malware, worm, bot, backdoor, spyware, rootkit**, ou de quaisquer outros que venham a ser criados), em decorrência da navegação na Internet pelo Usuário.

Em hipótese alguma, o sistema e seus colaboradores responsabilizam-se por eventuais danos diretos, indiretos, emergentes, especiais, imprevistos ou multas causadas, em qualquer matéria de responsabilidade, seja contratual, objetiva ou civil (inclusive negligência ou outras), decorrentes de qualquer forma de uso do serviço, mesmo que advertida a possibilidade de tais danos.

Tendo em vista que o serviço público digital ou sistema lida com informações pessoais, o usuário concorda que não usará robôs, sistemas de varredura e armazenamento de dados (como "**spiders**" ou "**scrapers**"), links escondidos ou qualquer outro recurso escuso, ferramenta, programa, algoritmo ou método coletor/extrator de dados automático para acessar, adquirir, copiar ou monitorar o serviço, sem permissão expressa por escrito do órgão.

Caso o usuário descumpra os Termos de Uso ou o Aviso de Privacidade, ou seja, investigado em razão de má conduta, o órgão poderá restringir seu acesso. O usuário também deverá responder legalmente por essa conduta.

8. Respeito aos direitos autorais

O uso comercial das expressões utilizadas em aplicativos como marca, nome empresarial ou nome de domínio, além dos conteúdos do serviço, assim como os programas, bancos de dados, redes, arquivos que permitem que o usuário acesse sua conta estão protegidos pelas leis e tratados internacionais de direito autoral, marcas, patentes, modelos e desenhos industriais.

Ao acessar o serviço público digital ou sistema, os usuários declaram que irão respeitar todos os direitos de propriedade intelectual e os decorrentes da proteção de marcas, patentes e/ou desenhos industriais, depositados ou registrados, bem como todos os direitos referentes a terceiros que porventura estejam, ou estiveram de alguma forma, disponíveis no serviço público digital ou sistema. O simples acesso ao serviço público digital ou sistema não confere aos usuários qualquer direito ao uso dos nomes, títulos, palavras, frases, marcas, patentes, imagens, dados e informações, dentre outras, que nele estejam ou estiveram disponíveis.

É vedada a utilização do serviço público digital ou sistema para finalidades comerciais, publicitárias ou qualquer outra que contrarie a finalidade para a qual foi concebida, conforme

definido neste documento, sob pena de sujeição às sanções cabíveis na Lei nº 9.610/1998, que protege os direitos autorais no Brasil.

Os visitantes e usuários assumem toda e qualquer responsabilidade, de caráter civil e/ou criminal, pela utilização indevida das informações, textos, gráficos, marcas, imagens, enfim, todo e qualquer direito de propriedade intelectual ou industrial do sistema.

9. Direitos do titular de dados pessoais

O usuário possui os seguintes direitos, entre outros, conferidos pela Lei Geral de Proteção de Dados Pessoais:

a) Direito de confirmação e acesso (art. 18, I e II): é o direito do usuário de obter do serviço a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento e, se for esse o caso, o direito de acessar os seus dados pessoais.

b) Direito de retificação (art. 18, III): é o direito de solicitar a correção de dados incompletos, inexatos ou desatualizados.

c) Direito à limitação do tratamento dos dados (art. 18, IV): é o direito do usuário de limitar o tratamento de seus dados pessoais, podendo exigir a eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei Geral de Proteção de Dados.

d) Direito de oposição (art. 18, § 2º): é o direito do usuário de, a qualquer momento, se opor ao tratamento de dados por motivos relacionados com a sua situação particular, com fundamento em uma das hipóteses de dispensa de consentimento ou em caso de descumprimento ao disposto na Lei Geral de Proteção de Dados.

e) Direito de não ser submetido a decisões automatizadas (art. 20, LGPD): o titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

O usuário poderá apresentar requerimento expresso ao Ministério da Defesa, com fundamento na Lei Geral de Proteção de Dados - LGPD, para exercício de seus direitos por meio da plataforma integrada de ouvidoria e acesso à informação (Fala.BR).

10. Responsabilidades da administração pública com os dados pessoais

A Administração Pública, no papel de custodiante das informações, deve cumprir todas as legislações inerentes de forma a respeitar a finalidade dos dados utilizados no serviço público digital ou sistema.

A Administração Pública manterá estes Termos de Uso e Aviso de Privacidade atualizados e por meio deste serviço público digital ou sistema, em atendimento ao princípio da publicidade estabelecido no art. 37, **caput**, da Constituição Federal.

A Administração pública se compromete a preservar a funcionalidade do serviço público digital ou sistema, utilizando um layout que respeite a usabilidade e navegabilidade, facilitando a navegação sempre que possível, exibindo as funcionalidades de maneira completa, precisa e suficiente, de modo que as operações realizadas no serviço público digital ou sistema sejam claras.

11. Compartilhamento de dados pessoas

A Administração Pública poderá, quanto às ordens judiciais de pedido de informações, compartilhar informações necessárias para investigações ou tomar medidas

relacionadas a atividades ilegais, suspeitas de fraude ou ameaças potenciais contra pessoas, bens ou sistemas que sustentam o serviço público digital ou sistema ou de outra forma necessária para cumprir com as obrigações legais. Caso ocorra, a Administração Pública notificará os titulares dos dados, salvo quando o processo estiver em segredo de justiça.

12. Aviso de Privacidade

O Aviso de Privacidade estabelecido pelo Ministério da Defesa e utilizado pelo serviço púbico digital "nome do serviço público digital ou sistema" trata da utilização de dados pessoais.

Esse Aviso específico faz parte de forma inerente do presente Termo de Uso, ressaltando-se que os dados pessoais mencionados por esse Serviço serão tratados nos termos da legislação em vigor.

Para mais informações acesse nosso aviso de privacidade apresentado ao final deste Termo de Uso.

13. Atualização

As regras e as condições previstas neste Termo de Uso poderão ser modificadas pelo Ministério da Defesa a qualquer momento, seja para adaptá-las a alterações legislativas supervenientes, seja para disponibilizar ao usuário novas funcionalidades ou mesmo suprimir e/ou modificar as já existentes.

Cabe ao usuário acessar periodicamente o presente Termo a fim de manter-se informado sobre possíveis atualizações.

As alterações e/ou atualizações terão vigência a partir da data de sua publicação no sítio eletrônico do serviço.

A última atualização deste o presente Termo é indicada na data constante de seu rodapé.

14. Informações para contato

Em caso de dúvidas relacionadas ao serviço público digital "nome do serviço público digital ou sistema", entre em contato através dos nossos canais de atendimento:

I - Problemas com a prestação do serviço: Ouvidoria do Ministério da Defesa através do site https://www.gov.br/defesa/pt-br/canais_atendimento/ouvidoria ou pelo telefone (61) 2023-9400.

II - Dúvidas sobre o tratamento de dados pessoais: Encarregado pelo tratamento de dados pessoais: encarregado@defesa.gov.br

Para apresentar requerimento expresso ao Ministério da Defesa, com fundamento na Lei de Proteção de Dados Pessoais - LGPD, para exercício de seus direitos utilize a plataforma integrada de ouvidoria e acesso à informação (Fala.BR).

15. Foro

Este Termo será regido pela legislação brasileira. Qualquer reclamação ou controvérsia com base neste Termo será dirimida perante a Justiça Federal.

Sem prejuízo de qualquer outra via administrativa ou judicial disponível, todos os titulares de dados pessoais têm direito a apresentar reclamação à Autoridade Nacional de Proteção de Dados - ANPD.

AVISO DE PRIVACIDADE

1. Definições

Para melhor compreensão deste documento, recomenda-se consultar as definições constantes do artigo 5º da Lei nº 13.709 de 14 de agosto de 2018 e do Glossário de Segurança da Informação, em especial consideram-se as seguintes definições:

I - Agentes de tratamento: O controlador e o operador.

II - Autoridade Nacional: Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

III - Banco de Dados: Conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

IV - Controlador: Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

V - Dado Pessoal: Informação relacionada a uma pessoa natural identificada ou identificável.

VI - Dado Pessoal Sensível: 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.

VII - 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.

VIII - Operador: Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

IX - Titular: Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

X - 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.

XI - Uso Compartilhado de Dados: Comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

2. Base Legal para tratamento de dados pessoais

Este Aviso de Privacidade foi elaborado em conformidade com a Lei Federal nº 12.965 de 23 de abril de 2014 (Marco Civil da Internet) e com a Lei Federal nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD).

A administração pública se compromete a cumprir as normas previstas na Lei Geral de Proteção de Dados Pessoais - LGPD, e respeitar seus princípios dispostos no Art. 6º:

I - **finalidade**: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - **adequação**: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - **necessidade**: limitação do 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;

IV - **livre acesso**: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - **qualidade dos dados**: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - **transparência**: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII - **segurança**: 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;

VIII - **prevenção**: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - **não discriminação**: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X - **responsabilização e prestação de contas**: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

3. Agentes de tratamento

As decisões referentes ao serviço público digital “nome do serviço público digital ou sistema” competem ao Ministério da Defesa no exercício das funções típicas de Controlador de dados pessoais.

As Forças Armadas são responsáveis pelo banco de dados deste serviço público digital exercendo, portanto, a controladoria conjunta dos dados pessoais e a responsabilidade sob o tratamento realizado.

Para esclarecimento de dúvidas sobre o tratamento de dados pessoais por este serviço público digital, poderá entrar em contato pelo e-mail encarregado@defesa.gov.br.

Para apresentar requerimento expresso ao Ministério da Defesa, com fundamento na Lei Geral de Proteção de Dados Pessoais - LGPD, para exercício de seus direitos utilize a plataforma integrada de ouvidoria e acesso à informação (Fala.BR).

Para maiores informações consulte: https://www.gov.br/defesa/pt-br/acesso-a-informacao/lei-geral-de-protecao-de-dados-pessoais-lgpd.

Se você está encontrando problemas com a prestação do serviço ou tem dúvidas sobre ele, não responda aos e-mails automáticos, entre em contato com a ouvidoria do Ministério

da Defesa através do site https://www.gov.br/defesa/pt-br/canais_atendimento/ouvidoria ou pelo telefone (61) 2023-9400.

4. Encarregado pelo tratamento de dados pessoais

Para o serviço público digital "nome do serviço público digital ou sistema", o responsável por atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados é o encarregado pelo tratamento de dados pessoais, cujos dados estão disponíveis em: https://www.gov.br/defesa/pt-br/acesso-a-informacao/lei-geral-de-protecao-de-dados-pessoais-lgpd.

Entre em contato com o encarregado pelo e-mail encarregado@defesa.gov.br para sanar quaisquer dúvidas sobre esta Política de Privacidade ou para obter mais informações sobre o tratamento dos dados realizado com fundamento na Lei Geral de Proteção de Dados Pessoais - LGPD.

5. Direitos do titular de dados pessoais

O titular de dados pessoais possui os seguintes direitos, conferidos pela Lei Geral de Proteção de Dados Pessoais - LGPD:

a) Direito de confirmação e acesso (art. 18, incisos I e II): é o direito do titular de dados de obter do serviço a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento e, se for esse o caso, o direito de acessar os seus dados pessoais.

b) Direito de retificação (art. 18, inciso III): é o direito de solicitar a correção de dados incompletos, inexatos ou desatualizados.

c) Direito à limitação do tratamento dos dados (art. 18, inciso IV): é o direito do titular de dados de limitar o tratamento de seus dados pessoais, podendo exigir a eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei Geral de Proteção de Dados Pessoais - LGPD.

d) Direito de oposição (art. 18, § 2º): é o direito do titular de dados de, a qualquer momento, opor-se ao tratamento de dados por motivos relacionados com a sua situação particular, com fundamento em uma das hipóteses de dispensa de consentimento ou em caso de descumprimento ao disposto na Lei Geral de Proteção de Dados Pessoais.

e) Direito de portabilidade dos dados (art. 18, inciso V): é o direito do titular de dados de realizar a portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial.

f) Direito de não ser submetido a decisões automatizadas (art. 20): o titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

6. Dados pessoais tratados neste sistema

A utilização, pelo usuário, de determinadas funcionalidades do serviço dependerá do tratamento dos seguintes dados pessoais informados diretamente no serviço público digital ou sistema:

Dado tratado	Forma de Coleta

Inserir lista dos dados pessoais tratados de acordo com o serviço ou sistema e a forma de coleta

Exemplos de dados pessoais:

a) Nome completo;

b) Nome social;

c) Data de nascimento;

d) Sexo;

e) Filiação;

f) Nacionalidade;

g) Naturalidade;

h) Número de inscrição no CPF;

i) Situação cadastral no CPF;

j) Estado civil;

k) Endereço de e-mail;

l) Endereço;

m) Número de telefone;

n) RG;

o) Dados do dispositivo (modelo de hardware, sistema operacional);

p) Localização do usuário;

q) Registro de acesso;

r) Foto do usuário.

Exemplos de como os dados podem ser coletados:

a) Obtido de terceiros (exemplo: *Login* Único, Google etc.);
b) Informado pelo usuário;
c) Obtido ao utilizar o serviço;
d) Câmera do dispositivo;
e) *Cookies*;
f) Localização do dispositivo;
g) Microfone do dispositivo;

h) Obtido pelo dispositivo de acesso, após autorização do usuário.

Descrever a finalidade para a qual o tratamento de dados pessoais é realizado

7. Decisões automatizadas

Caso sejam realizadas decisões automatizadas, descrever tais decisões e sua finalidade, bem como a forma de recorrer de tais decisões.

8. Compartilhamento de dados pessoais

A Administração Pública poderá, quanto às ordens judiciais de pedido de informações, compartilhar informações necessárias para investigações ou tomar medidas relacionadas a atividades ilegais, suspeitas de fraude ou ameaças potenciais contra pessoas, bens ou sistemas que sustentam o sistema ou de outra forma necessária para cumprir com as obrigações legais. Caso ocorra, a Administração Pública notificará os titulares dos dados, salvo quando o processo estiver em segredo de justiça.

Se forem compartilhados justificar a necessidade e a forma de compartilhamento.

9. Transferência Internacional de dados pessoais

Os dados pessoais do usuário não são transferidos internacionalmente em nenhuma hipótese.

Se forem transferidos justificar a necessidade e a forma de transferência internacional.

10. Segurança no tratamento dos dados pessoais

O Ministério da Defesa, por intermédio do Comando da Marinha, do Exército e da Aeronáutica, se compromete a aplicar as medidas técnicas e organizacionais aptas a proteger o serviço público digital “nome do serviço público digital ou sistema” e os dados pessoais nele armazenados de acessos não autorizados e de situações de destruição, perda, alteração ou difusão de tais dados.

Para a garantia da segurança, serão adotadas soluções que levem em consideração: as técnicas adequadas; os custos de aplicação; a natureza, o âmbito, o contexto e as finalidades do tratamento; e os riscos para os direitos e liberdades do usuário.

O serviço utiliza criptografia em toda comunicação que realiza, de forma a fornecer segurança às informações que trafegam entre o usuário e o servidor, e evitar que acessos indevidos ocorram.

No entanto, se exime de responsabilidade por culpa exclusiva de terceiros, como em caso de ataque de *hackers* ou *crackers*, ou culpa exclusiva do usuário, como no caso em que ele mesmo transfira seus dados a terceiro.

A violação de dados pessoais é uma violação de segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso não autorizado a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.

Por fim, o sistema trata os dados pessoais do usuário com confidencialidade, dentro dos limites legais.

11. Utilização de cookies

Cookies são pequenos arquivos de texto enviados pelo site ao computador do usuário e que nele ficam armazenados, com informações relacionadas à navegação do site.

Por meio dos cookies, pequenas quantidades de informação são armazenadas pelo navegador do usuário para que o servidor do serviço possa lê-las posteriormente. Podem ser armazenados, por exemplo, dados sobre o dispositivo utilizado pelo usuário, bem como seu local e horário de acesso ao site.

É importante ressaltar que nem todo cookie contém dados pessoais do usuário, já que determinados tipos de *cookies* podem ser utilizados somente para que o serviço funcione corretamente. Porém, quando registram informações que permitam identificar o usuário, tais informações também são consideradas dados pessoais e todas as regras previstas neste Aviso de Privacidade também são aplicáveis aos *cookies*.

Este sistema, para fins de funcionamento envia cookies de sessão, que permanecem em seu dispositivo apenas até fechar o navegador.

Relacionar outros cookies que sejam utilizados.

Exemplos de *cookies*

Nome do *Cookie*	**Finalidade da utilização**
Lgpd_cookie_status (exemplo)	Registrar o aceite do banner de cookies da página inicial
I18N_LANGUAGE (exemplo)	Registrar o idioma em que o site deve ser exibido
Browserupdateorg (exemplo)	Notificar o usuário quando ele usa um navegador antigo ou incompatível

12. Tratamento posterior dos dados para outras finalidades

Informações sobre inserir dados pessoais utilizados para utilização posteriores, dentre outros, podem ser utilizados para melhoria contínua dos serviços e aprimoramento da experiência do usuário no âmbito do inserir o “serviço público digital ou sistema”.

Caso o titular de dados pessoais inserir o serviço público digital ou sistema opte por excluir os seus dados, eles serão anonimizados. Os dados anonimizados poderão ser utilizados futuramente para geração de estatísticas, de forma a melhorar os procedimentos do serviço inserir o serviço público digital ou sistema. Também podem ser utilizados para fins de pesquisa por órgãos especializados no assunto. Podem, igualmente, ser utilizados de maneira agregada para divulgação de informações através de meios de comunicação, e em publicações científicas e educacionais.

13. Atualização

As regras e as condições previstas neste Aviso de Privacidade poderão ser modificadas pelo Ministério da Defesa a qualquer momento, seja para adaptá-las a alterações legislativas supervenientes, seja para disponibilizar ao usuário novas funcionalidades ou mesmo suprimir e/ou modificar as já existentes.

Cabe ao usuário acessar periodicamente o presente Aviso a fim de manter-se informado sobre possíveis atualizações.

As alterações e/ou atualizações terão vigência a partir da data de sua publicação no sítio eletrônico do serviço.

A última atualização deste o presente Aviso é indicada na data constante de seu rodapé.

MINISTÉRIO DA DEFESA

PROGRAMA DE GESTÃO EM PRIVACIDADE

ANEXO D

PROCEDIMENTOS EM CASO DE INCIDENTES ENVOLVENDO DADOS PESSOAIS

1. INTRODUÇÃO

Incidente de segurança com dados pessoais pode ser entendido como qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito, que resulte em destruição, perda, alteração, vazamento ou, ainda, qualquer forma de tratamento de dados inadequada ou ilícita, que possa ocasionar risco para os direitos e liberdades do titular dos dados pessoais[12].

Visando evitar a ocorrência de incidentes de segurança com dados pessoais, 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. Tais medidas de segurança deverão ser observadas desde a concepção do produto ou serviço até a sua execução[13].

Neste sentido, a Diretriz para a Proteção de Dados Pessoais no Ministério da Defesa estabelece que cabe ao responsável pela unidade organizacional onde os dados pessoais são tratados implementar medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais, ou não, de eliminação, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, nos termos da Lei nº 13.709, de 14 de agosto de 2018, por meio das seguintes ações:

a) implementação do previsto na Política de Segurança da Informação;

b) adoção de mecanismos de segurança e privacidade, desde a concepção de novos produtos ou serviços (*security by design* e *privacy by design*);

c) elaboração de um plano de resposta a incidentes identificados no relatório de impacto;

d) avaliação dos sistemas e bancos de dados em que houver tratamento de dados pessoais ou tratamento de dados sensíveis, bem como suas eventuais integrações com outros sistemas, submetendo os riscos identificados, quando não passíveis de tratamento, à apreciação do Gestor de Segurança da Informação, para as orientações necessárias;

e) análise da segurança das hipóteses de compartilhamento de dados pessoais; e

f) realização de treinamentos.

Estabelece, ainda, que as unidades organizacionais responsáveis pelo tratamento de dados pessoais devem monitorar preventivamente os eventos relacionados no relatório de impacto à proteção de dados pessoais, visando evitar incidentes envolvendo dados pessoais.

[12] https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_resposta_incidentes.pdf

[13] art. 46 da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD)

2. PROCEDIMENTOS EM CASO DE INCIDENTE

Em caso de incidente que coloque em risco a segurança de dados pessoais, devem ser realizados alguns procedimentos específicos. São eles:

I - **Avaliar internamente o incidente** com o objetivo de obter informações iniciais sobre impacto do evento. A unidade organizacional responsável pelo ativo de informação que foi alvo do incidente deverá reunir as informações que contemplem os seguintes aspectos:

a) vulnerabilidade explorada no evento;

b) fonte dos dados pessoais (meio pelo qual foram obtidos os dados pessoais, tais como preenchimento de formulário eletrônico ou não eletrônico por parte do titular, *API*, uso compartilhado de dados, *XML* e *cookies*)

c) natureza e categoria dos dados pessoais (dados pessoais sensíveis ou de crianças e adolescentes);

d) extensão do incidente (quantidade de titulares de dados pessoais afetados; categoria e quantidade de dados afetados);

e) avaliação do impacto ao titular (avaliar quais são os impactos que o incidente gerou ou poderá gerar aos titulares);

f) avaliação do impacto para o Ministério da Defesa (avaliar os impactos que o incidente pode gerar ao Ministério da Defesa, como perda de confiabilidade do cidadão, sanções da Autoridade Nacional de Proteção de Dados - ANPD, ações judiciais, dano à imagem da instituição em âmbito nacional e internacional, prejuízo em contratos com fornecedores, e impacto total ou parcial nas atividades desenvolvidas pelo Ministério da Defesa);

g) evidências do incidente, tais como: todos os logs dos sistemas internos e externos envolvidos no incidente; interações do time envolvido e todas as medidas adotadas; eventuais contratações de ferramentas e equipes de especialistas e auditores para atuação pontual no incidente a ser tratado; atas das reuniões sobre a ocorrência do incidente, etc.

O Apêndice “A” apresenta um formulário a ser preenchido para apoiar a avaliação interna do incidente.

II - **Comunicar ao Gestor de Segurança da Informação e ao Encarregado pelo tratamento de dados pessoais:** Cabe a unidade organizacional responsável pelo ativo de informação que foi alvo do incidente, no prazo máximo de vinte e quatro horas, comunicar o incidente, com esclarecimento da natureza do incidente e das medidas adotadas para a apuração das suas causas e a mitigação de novos riscos e dos impactos causados aos titulares dos dados, via e-mail e TI Ajudo ou SUPER.GOV.BR ao Gestor de Segurança da Informação, e caso envolva dados pessoais, ao Encarregado pelo tratamento de dados pessoais.

III - **Comunicar a Alta Administração a ocorrência do incidente:** O Gestor de Segurança da Informação comunicará o incidente para a Alta Administração, e, caso envolva dados pessoais, avaliará junto com o Encarregado pelo tratamento de dados pessoais a necessidade de comunicar o fato à Autoridade Nacional de Proteção de Dados - ANPD.

IV - **Comunicar à ANPD e ao titular de dados pessoais** (conforme art. 48 da Lei Geral de Proteção de Dados Pessoais - LGPD: O Encarregado pelo tratamento de dados pessoais encaminhará a ocorrência do incidente para Autoridade Nacional de Proteção de Dados - ANPD, caso possa acarretar risco ou dano relevante aos titulares.

A Autoridade Nacional de Proteção de Dados - ANPD recomenda que o prazo razoável para a comunicação de incidente seja de dois dias úteis, mesmo que a comunicação ocorra de forma preliminar e venha a ser complementada oportunamente. Os procedimentos para comunicação de incidente à Autoridade Nacional de Proteção de Dados - ANPD podem ser verificados em https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca.

Recomenda também que os controladores tenham cautela quanto ao julgamento acerca da relevância dos riscos e danos referentes ao incidente e, em caso de dúvida, realizem a

comunicação do incidente o mais breve possível para que não ocorra eventual descumprimento daLei Geral de Proteção de Dados Pessoais - LGPD.

V - **Comunicar à Equipe de Prevenção e Tratamento de Incidentes: Caso o incidente envolva** a rede computacional da administração central do Ministério da Defesa - ACMD, aquele que tiver conhecimento inicial deverá imediatamente comunicar à Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR por meio do e-mail abuse@defesa.gov.br. Caso necessário a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR providenciará a comunicação ao CTIR.GOV, observado o previsto na Norma Complementar nº 21 /IN01/DSIC/GSIPR[14].

VI - **Elaborar o Relatório de Impacto à Proteção de Dados Pessoais - RIPD**: A unidade organizacional responsável pelo ativo de informação com apoio do Encarregado pelo tratamento de dados pessoais deverá elaborar o RIPD caso o incidente envolvendo dados pessoais represente risco ou dano relevante aos titulares, observados os artigos art. 4º, inciso III, 31, 32 e 38 da Lei Geral de Proteção de Dados Pessoais - LGPD, conforme modelo do Anexo B deste Programa de Gestão em Privacidade - PGP.

A Autoridade Nacional de Proteção de Dados - ANPD pode solicitar o Relatório de Impacto à Proteção de Dados Pessoais - RIPD para análise, com o propósito de: avaliar as ações tomadas durante um incidente em que dados pessoais tenham sido expostos ou comprometidos; publicar e atualizar normas referentes à proteção de dados; cumprir o princípio da responsabilização (art. 6º, inciso X da Lei Geral de Proteção de Dados Pessoais - LGPD); utilizá-lo como subsídio para eventuais questionamentos, facilitando a comprovação de conformidade.

VII - Emitir o relatório final do incidente: Ao final do tratamento do incidente, todos os envolvidos, sob coordenação do Gestor de Segurança da Informação contribuirão para elaboração do relatório final com todas as informações coletadas, as ações realizadas para o tratamento efetivo do evento e as considerações necessárias para promover a melhoria contínua no atendimento de incidentes e para atualizar o Relatório de Impacto à Proteção de Dados Pessoais - RIPD.

A figura abaixo apresenta os procedimentos acima relacionados:

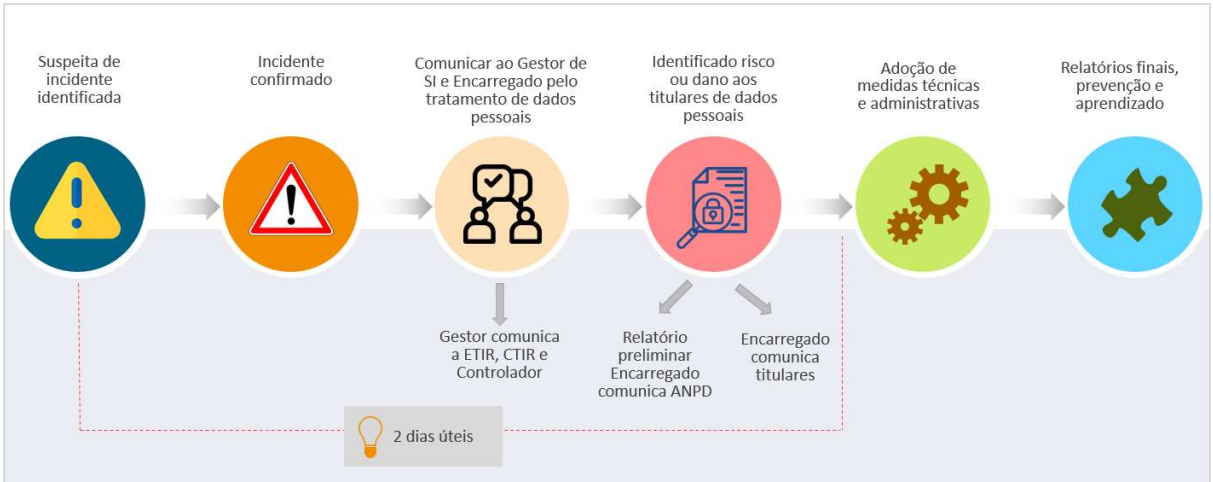

Figura 1: Procedimentos em caso de incidente de segurança envolvendo dados pessoais

14 https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=10/10/2014&jornal=1&pagina=5&totalArquivos=224

3. RESPOSTA A INCIDENTES ENVOLVENDO DADOS PESSOAIS

A resposta a incidentes de segurança envolvendo dados pessoais visa minimizar os impactos causados pela violação na segurança de dados pessoais.

Ao confeccionar um Relatório de Impacto à Proteção de Dados Pessoais - RIPD, a unidade finalística responsável pelo tratamento de dados pessoais consegue identificar os riscos envolvidos e pode planejar ações para minimizar os impactos em caso de ocorrência.

Esse planejamento deve ser consubstanciado num Plano de Resposta que oriente o emprego de medidas técnicas e administrativas para enfrentar a situação adversa.

O Guia de Resposta a Incidentes de Segurança[15] informa que segundo o *National Institute of Standards and Technology - NIST*[16], o processo de resposta a incidentes possui quatro fases:

a) Preparação: criar e treinar equipes para atuar na resposta a incidentes, além de limitar o número de incidentes, selecionando e implementando controles com base em avaliações de risco.

b) Detecção e análise de incidentes: adotar meios para detecção de incidentes e analisar tais eventos, buscando documentar, priorizar e notificar; esta fase também pode ser executada em conjunto com a fase posterior.

c) Contenção, erradicação e recuperação: fase em que são implementadas ações para contenção, erradicação e recuperação do incidente, bem como são identificadas as origens de ataques e coletadas as evidências.

d) Atividades pós-incidente: a entidade deve realizar atividades para melhorar o tratamento de novos incidentes.

Figura 2: Ciclo de Resposta a Incidentes - NIST

Criar plano de resposta para os incidentes identificados no RIPD possibilita que se oriente o trabalho caso venha a ocorrer e permite dimensionar os impactos de acordo com a vulnerabilidade que possa ser explorada, contribuindo para interromper a violação na segurança de dados pessoais com a brevidade que o assunto requer, bem como orientar como os dados poderão ser recuperados, caso possível, ou as medidas a serem adotadas.,

O apêndice B apresenta um modelo de plano de resposta a incidentes envolvendo dados pessoais.

[15] https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_resposta_incidentes.pdf
[16] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf página 21

APÊNDICE A DO ANEXO D

FORMULÁRIO PARA APOIAR A AVALIAÇÃO INTERNA DO INCIDENTE

Dados do notificante:

Secretaria / Departamento: *[Resposta]*

Nome do notificante: *[Resposta]*

E-mail: *[Resposta]*

Telefone: *[Resposta]*

Incidente de segurança

Descreva de forma resumida como o incidente de segurança com dados pessoais ocorreu, mencionando qual vulnerabilidade foi explorada no evento

[Resposta]

Quais as fontes de dados envolvidas no inciente?

☐Formulário ou documento em meio físico

☐Formulário eletrônico (excel, pdf, ...).

☐Banco de dados estruturado

☐Base de dados não estruturada

☐Sites (cookies, cadastros on line, ...)

☐Acesso externo (*API, XML*, ...)

☐Outros. Descrever: *[Resposta]*

Quando o incidente ocorreu?

[Data e hora]

☐Não tenho conhecimento. Justifique: *[Resposta]*

☐Não tenho certeza. Justifique: *[Resposta]*

Quando teve ciência do incidente de segurança?

[Data e hora]

Descreva como teve ciência do incidente de segurança.

[Resposta]

Se o incidente não foi comunicado de forma imediata, ao Gestor de Segurança da Informação e ao Encarregado pelo tratamento de dados pessoais, após a sua ciência, justifique os motivos da demora.

[Resposta]

Qual a natureza dos dados afetados?

☐Origem racial ou étnica.

☐Convicção religiosa.

☐Opinião política.

☐Filiação a sindicato.

☐Filiação a organização de caráter religioso, filosófico ou político.

☐Dado referente à saúde.

☐Dado referente à vida sexual.

☐Dado genético ou biométrico.

☐Dado de comprovação de identidade oficial (Por exemplo, nº RG, CPF, CNH).

☐Dado financeiro.

☐Nomes de usuário ou senhas de sistemas de informação.

☐Dado de geolocalização.

Outros: *[Resposta]*

Qual a categoria dos titulares afetados?

☐Funcionários ou pessoas com vínculo profissional com o MD

☐Prestadores de serviço

☐Visitantes

☐Usuários

☐Pacientes de serviço de saúde

☐Crianças ou adolescentes

Outros: *[Resposta]*

Extensão do incidente. Qual a quantidade aproximada de titulares afetados e a quantidade (volume) de dados afetados?

[Resposta]

Medidas de segurança utilizadas para a proteção dos dados

Quais medidas de segurança, técnicas e administrativas, foram tomadas para prevenir a ocorrência do incidente de segurança?

[Resposta]

Quais medidas de segurança, técnicas e administrativas, foram tomadas após a ciência do incidente de segurança?

[Resposta]

Quais medidas de segurança, técnicas e administrativas, foram ou serão adotadas para reverter ou mitigar os efeitos do prejuízo do incidente de segurança aos titulares dos dados?

[Resposta]

Possui relatório de impacto à proteção de dados pessoais referente ao tratamento dos dados pessoais afetados pelo incidente?

[Resposta]

Avaliação do impacto aos titulares

Risco ou dano relevante aos titulares:

☐O incidente de segurança pode acarretar risco ou dano relevante aos titulares.

☐Não tenho certeza sobre o nível de risco do incidente de segurança.

Quais as prováveis consequências do incidente de segurança para os titulares afetados?

[Resposta]

Avaliação do impacto ao Ministério da Defesa

Os dados pessoais eram compartilhados com outros órgãos?

[Resposta]

Considerando os titulares afetados, na sua avaliação, o incidente pode trazer consequências transfronteiriças?

[Resposta]

Assinale os impactos que o incidente pode causar para o Ministério da Defesa:

☐perda de confiabilidade do cidadão

☐dano à imagem do Ministério da Defesa em âmbito Nacional e internacional

☐prejuízo em contratos firmados pelo Ministério da Defesa

☐inoperância total ou parcial das atividades desenvolvidas pelo Ministério da Defesa

☐sanções pela Autoridade Nacional de Proteção de Dados - ANPD

APÊNDICE B DO ANEXO D

MODELO DE PLANO DE RESPOSTA A INCIDENTES ENVOLVENDO DADOS PESSOAIS

1. INTRODUÇÃO

A Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais - LGPD, tem como um de seus pilares a adoção de 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 outra forma de tratamento inadequado ou ilícito.

2. ABRANGÊNCIA E VIGÊNCIA

Este Plano de Resposta a Incidentes envolvendo dados pessoais estabelece o procedimento para a gestão de incidente de segurança da informação que envolva dados de pessoa natural identificada ou identificável que são tratados pelo Ministério da Defesa, no âmbito da <Secretaria / Departamento>, visando prevenir a ocorrência de incidentes e minimização eventuais efeitos relacionados a incidentes.

3. TERMOS E DEFINIÇÕES

<relacionar os termos e definições expressos na Lei Geral de Proteção de Dados Pessoais - LGPD e no glossário de segurança da informação do Gabinete de Segurança da Informação da Presidência da República[17] que facilitem a compreensão do tema>.

4. PAPÉIS E RESPONSABILIDADES

Cada unidade finalística tem responsabilidades quando da ocorrência ou mera suspeita de um Incidente, devendo comunicar, imediatamente, o fato ao Gestor de Segurança da Informação, que estabelecerá uma equipe de resposta a incidentes.

Os principais papéis envolvidos em violações de dados pessoais são:

a) Notificador: pessoa ou sistema de monitoração que notifica o incidente;

b) Acionador(es): responsável pelo recebimento das notificações e realização do tratamento inicial (triagem) do incidente;

c) Grupo de Resposta a Incidentes envolvendo dados pessoais: grupo de pessoas, com acessos, habilidades, responsabilidades, treinamento e conhecimentos para responder os incidentes. O grupo será designado de acordo com as especificidades de cada incidente, sendo coordenado pelo Gestor de Segurança da Informação e composto por pessoas que detenham expertise para a abordagem do tema ou cujos processos tenham sido afetados pelo incidente.

d) Responsável por Sistema: pessoa, com capacidade de propor soluções de resposta, bem como, autorizar ou vetar procedimentos de emergência;

e) Responsável por Processo ou Negócio: coordenador-geral ou coordenador com capacidade de propor soluções de resposta para a equipe de tratamento de incidentes;

f) Equipe de Prevenção, Tratamento e Resposta a Incidentes em Redes Computacionais da administração central do Ministério da Defesa - ETIR-ACMD: instituída conforme

[17] https://www.gov.br/gsi/pt-br/assuntos/dsi/glossario-de-seguranca-da-informacao-1

Portaria GM-MD nº 3.381, de 16 de agosto de 2021, que tem por missão receber, analisar e responder notificações e atividades relacionadas a incidentes de segurança da informação e comunicações em sistemas computacionais no âmbito da rede administrativa da administração central do Ministério da Defesa, atuando também de forma proativa, com o objetivo de minimizar vulnerabilidades e ameaças que possam comprometer a missão da instituição, em consonância com as atividades de resposta e tratamento a incidentes em redes, tais como: recuperação de sistemas, análise de ataques e intrusões, cooperação com outras equipes, participação em fóruns e redes nacionais e internacionais;

g) Comitê de Segurança da Informação: instituído pela Portaria GM-MD nº 3.247, de 8 de junho de 2022, com a finalidade de assessorar o Ministro de Estado da Defesa nas atividades relacionadas à Segurança da Informação no âmbito da administração central do Ministério da Defesa, observado o disposto no Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação - PNSI;

h) Gestor de Segurança da Informação: designado conforme Portaria GM-MD n° 3.910, de 18 de julho de 2022; e

i) Encarregado pelo Tratamento de Dados Pessoais: designado conforme Portaria GM-MD n° 1.648, de 9 de abril de 2021.

5. INCIDENTES DE SEGURANÇA ENVOLVENDO DADOS PESSOAIS EM MEIO DIGITAL

5.1. Detecção

A identificação de qualquer Incidente de Segurança é aspecto chave para a boa implementação de um Plano de Respostas a Incidentes.

São várias as formas de identificação. Desta forma, todos devem atentar-se, principalmente, aos sinais mais comuns que podem desencadear um Incidente, como incidentes em redes, perda ou furto de documentos, arquivos ou dispositivos*, phishing, malware*, instabilidades de sistemas, entre outras. Além disto, ferramentas de monitoramento, eventos de log, mensagens de erro de firewalls e softwares de segurança, entre outros contribuem para detectar incidentes.

Além disto, a comunicação inicial do incidente pode ser proveniente de qualquer fonte, tais como: e-mails, sistemas, telefone, “Fale Conosco”, Plataforma “Fala.BR”, TI Ajudo.

Portanto, deve haver um trabalho maciço de sensibilização e capacitação de servidores/funcionários/colaboradores, para que, proativamente, esses tenham a capacidade de identificar e informar eventual incidente ou vazamento de dados pessoais, de que tenham conhecimento.

Uma vez detectado um Incidente ou detectada a mera suspeita de um Incidente, o NOTIFICADOR deverá comunicar imediatamente ao ACIONADOR, preferencialmente por meio do TI AJUDO. Para tanto, orienta-se por preencher o formulário para apoiar a avaliação interna do incidente, com as informações que dispor inicialmente. O preenchimento completo do formulário será realizado em etapas posteriores.

Na medida do possível, essa comunicação deverá conter:

a) a hora e a data em que a suspeita do Incidente foi descoberta;

b) o tipo de informações envolvidas;

c) a causa e a extensão do Incidente;

d) o contexto do ocorrido; e

e) qualquer informação adicional que sirva para facilitar o entendimento do evento, suas causas e consequências.

5.2. Triagem

O ACIONADOR deve fazer a avaliação preliminar ou contatar imediatamente outro ACIONADOR em condições de realizar a referida avaliação, descartando as notificações nulas ou claramente improcedentes, tomando os devidos cuidados de registrar os motivos do descarte.

Na avaliação preliminar, devem ser buscadas informações sobre os sistemas que foram possivelmente impactados, sua criticidade, quais os danos aparentes e o risco da situação se agravar se não houver resposta imediata.

Conforme a avaliação preliminar, incidentes que não envolvem sistemas online e que seguramente não apresentam riscos relevantes aos titulares de dados pela falta de ação imediata podem ser reencaminhados para trâmites regulares da Equipe de Tratamento e Prevenção de Incidentes em Redes Computacionais. Identificada a existência de dados pessoais, o Encarregado pelo Tratamento de Dados Pessoais também deve ser notificado.

Em caso de incidentes que exigem resposta imediata ou melhor avaliação, o Gestor de Segurança da Informação deve ser acionado e passa-se para as fases seguintes.

5.3. Avaliação

Nesta fase deve ser iniciada uma avaliação mais detalhada do incidente, classificando-o e definindo a sua criticidade. Deve-se procurar identificar a causa do incidente, atores e ações envolvidas, vulnerabilidades exploradas, visando determinar ações para as demais fases. Pode ser importante engajar especialistas dos setores afetados para colaborar.

O formulário para apoiar a avaliação interna do incidente deverá ser completamente preenchido para subsidiar o processo de análise.

5.3.1 São exemplos de classificação de incidentes:

a) Conteúdo abusivo: spam, assédio, etc;

b) Código malicioso: *worm*, vírus, *trojan, spyware, scripts*;

c) Prospecção por informações: varredura, *sniffing*, engenharia social;

d) Tentativa de intrusão: tentativa de exploração de vulnerabilidades, tentativa de acesso lógico;

e) Intrusão: acesso lógico indesejável. comprometimento de conta de usuário, comprometimento de aplicação;

f) Indisponibilidade de serviço ou informação: negação de serviço, sabotagem;

g) Segurança da informação: acesso não-autorizado à informação, modificação não autorizada da informação;

h) Fraude: violação de direitos autorais, fingir ou falsificar identidade pessoal ou institucional, uso de recursos de forma não-autorizada; e

i) Outros: incidente não categorizado.

5.3.2 Em caso de vários incidentes, é importante definir uma ordem de atendimento de acordo com a urgência de tratamento e o impacto nas áreas de negócio. A criticidade do incidente pode ser definida de acordo com as seguintes classificações:

a) Alto (Impacto Grave) - Incidente que afeta sistemas relevantes ou informações críticas, com potencial para gerar impacto negativo sobre a instituição;

b) Médio (Impacto Significativo) - Incidente que afeta sistemas ou informações não críticas, sem impacto negativo à instituição; e

c) Baixo (Impacto Mínimo) - Possível incidente, sistemas não críticos.

O impacto da violação de dados também pode ser mensurado empregando a tabela a seguir:

Volume de Dados Pessoais expostos	Alto	Alta Gravidade	Alta Gravidade	Alta Gravidade
	Médio	Média Gravidade	Alta Gravidade	Alta Gravidade
	Baixo	Baixa Gravidade	Média Gravidade	Média Gravidade
		Baixa	Média	Alta
		Sensibilidade dos Dados Pessoais afetados		

Volume de Dados Pessoais expostos	
Criticidade	Descrição
Alto	Volume de Dados Pessoais afetado superior a 10% da base de dados violada.
Médio	Volume de Dados Pessoais afetado inferior a 10% e superior a 2% da base de dados violada.
Baixo	Volume de Dados Pessoais afetado inferior a 2% da base de dados violada.

Sensibilidade dos Dados Pessoais afetados	
Criticidade	Descrição
Alta	Dados Pessoais de crianças/ adolescentes, dados Pessoais Sensíveis ou que possam gerar discriminação ao titular.
Média	Dados Pessoais imediatamente identificáveis (Ex.: nome, e-mail, CPF, endereço), combinados, ou não, com informações comportamentais (Ex.: histórico de atividades, preferências).
Baixa	Dados anonimizados, Dados Pessoais pseudonimizados (desde que a chave de desanonimização também não tenha sido comprometida), Dados Pessoais de difícil identificação (Ex.: IP)

De acordo com a classificação definida, o Gestor de Segurança da Informação poderá orientar a tomada das seguintes ações, simultaneamente ou, quando não for possível, em rápida sucessão:

I - Baixa Gravidade:

a) tão logo tenha ciência, trabalhar prioritariamente na resolução do incidente;

b) tomar as medidas adequadas para minimizar os efeitos causados pelo Incidente e para promover sua rápida correção;

c) comunicar ao Comitê de Segurança da Informação;

d) comunicar as áreas envolvidas, que deverão estar à disposição do Grupo de Resposta a Incidentes envolvendo dados pessoais;

e) uma vez que as medidas de resolução sejam tomadas, documentar o incidente; e

f) reunir-se para analisar o incidente e antecipar, prevenir e melhor identificar incidentes semelhantes no futuro, devendo esta reunião ser transcrita em relatório, que deverá ser apresentada ao Comitê de Segurança da Informação.

II - Média Gravidade:

a) tão logo tenha ciência, trabalhar de forma exclusiva na resolução do incidente;

b) tomar as medidas imediatas para minimizar os efeitos causados pelo Incidente e para promover sua rápida correção e, se a correção não for possível de forma imediata, deve adotar as medidas temporárias para minimização de riscos;

c) comunicar o Comitê de Segurança da Informação e a Equipe de Prevenção, Tratamento e Resposta a Incidentes em Redes Computacionais;

d) comunicar as áreas envolvidas, que deverão estar à disposição para atender, com prioridade, o Grupo de Resposta a Incidentes envolvendo dados pessoais;

e) uma vez que as medidas de resolução sejam tomadas, documentar o Incidente, o mais breve possível;

f) reunir-se o mais breve possível para analisar o incidente e antecipar, prevenir e melhor identificar Incidentes semelhantes no futuro, devendo esta reunião ser transcrita em ata documentada, que deverá ser apresentada ao Comitê de Segurança da Informação; e

g) realizar, imediatamente, treinamento interno com as áreas afetadas para conscientizar os seus colaboradores sobre o incidente e medidas preventivas.

III - Alta Gravidade:

a) tão logo tenha ciência, trabalhar de forma exclusiva na resolução do incidente;

b) imediatamente comunicar os diretores responsáveis pelas áreas envolvidas, os quais, em conjunto com outra pessoa de cada uma das respectivas áreas envolvidas, devem atuar de forma exclusiva no suporte ao Grupo de Resposta a Incidentes envolvendo dados pessoais e à Equipe de Prevenção, Tratamento e Resposta a Incidentes em Redes Computacionais;

c) uma vez que as medidas de resolução sejam tomadas, documentar o incidente, imediatamente;

d) reunir-se, imediatamente, para avaliar o incidente e antecipar, prevenir e melhor identificar Incidentes semelhantes no futuro, devendo esta reunião ser transcrita em relatório, que deverá ser apresentada ao Comitê de Segurança da Informação;

e) realizar, imediatamente, treinamento interno para conscientizar sobre o incidente e medidas preventivas; e

f) comunicar, imediatamente, os Colaboradores internos sobre medidas preventivas.

5.4. Contenção, erradicação e recuperação

Os responsáveis pelos sistemas/processos impactados devem ser acionados para se manifestarem sobre os procedimentos de resposta, contenção, erradicação e recuperação.

O objetivo das medidas de contenção e erradicação é limitar o dano e isolar os sistemas afetados para evitar mais danos. Aqui, conforme a necessidade e a autorização obtida, poderá ser realizado o desligamento dos sistemas inteiros ou de funcionalidades especificas e colocados avisos de indisponibilidade para manutenção. Todos os cuidados devem ser adotados para não impactar evidências que poderiam ser usadas para identificar autoria, origem e método usado para quebrar a segurança.

Em caso de incidente envolvendo máquinas virtuais, deve ser feito snapshot (registro do estado de um arquivo, aplicação ou sistema em um certo ponto no tempo) para posterior análise.

Em se tratando de incidentes não relacionados a recursos computacionais, mas essencialmente de atividade humana, os procedimentos podem envolver sindicância administrativa, processo administrativo disciplinar, entre outras medidas dispostas na legislação aplicável ao caso.

A recuperação é o conjunto de medidas para restaurar os serviços completamente, mas pode ser feita de forma gradual, conforme viabilidade e decisão do responsável pelo sistema/processo.

Pode ser necessário o desenvolvimento e instalação de atualizações de aplicação ou do Sistema Operacional, ou elaboração de novas rotinas processuais. De uma forma geral:

a) Preparação**:** Uma resposta a um incidente deve ser decisiva e executada prontamente. Como há pouco espaço para equívocos, é essencial que as práticas de emergência sejam exercitadas e os tempos de resposta medidos. Desta forma, é possível desenvolver uma metodologia que estimule a agilidade e a exatidão, minimizando o impacto da indisponibilidade de recursos e os potenciais danos causados pelo comprometimento do sistema/processos.

b) Contenção: Após a identificação de um incidente, o mesmo deve ser contido e, se for o caso, isolado, para que outros sistemas/processos não sejam afetados, evitando maiores danos ao ambiente. Essa etapa inclui a contenção de curto prazo, backup do sistema, contenção a longo prazo, dentre outros. É importante que, durante a etapa de contenção, ocorra simultaneamente a adoção de medidas que permitam a documentação e o registro do incidente, devendo ser evitado que evidências e provas do ocorrido sejam destruídas ou perdidas.

c) Erradicação: Após a contenção da ameaça, a próxima etapa consiste da remoção da ameaça e restauração dos sistemas/processos afetados para que retornem ao seu estado original antes do incidente.

d) Recuperação: Nesta etapa, os sistemas/processos afetados retornarão, após testes e validações, ao ambiente de produção, ou, ao habitual andamento, com vistas a garantir que nenhuma ameaça permaneça. Caso exista Plano de Continuidade de Negócio dos sistemas impactados, eles devem ser utilizados. A recuperação é o conjunto de medidas para restaurar os serviços completamente, mas pode ser feita de forma gradual, conforme viabilidade e decisão do responsável pelo sistema. Para a recuperação devem ser tomadas medidas identificadas na avaliação, tais como restauração de backups, clonagem de máquinas virtuais, reinstalação de sistemas. Pode ser necessário o desenvolvimento e instalação de atualizações de aplicação ou do Sistema Operacional, por isso esta fase pode ser prolongada, de acordo com a priorização dada.

5.5. Lições aprendidas

Esta última etapa visa atualizar o Plano de Respostas a Incidentes com as ações realizadas para tratar o incidente, contribuindo para o aprendizado da equipe e facilitando as próximas atuações em futuros incidentes.

Com o incidente contido e sua resolução encaminhada, o Grupo de Resposta a Incidentes envolvendo dados pessoais deverá agendar e conduzir uma reunião de Lições Aprendidas, com convidados a seu critério, com o objetivo de discutir erros e dificuldades encontradas, propor melhorias para os sistemas e processos, validar a eficácia deste Plano de Resposta a Incidentes e subsidiar a documentação do incidente, incluindo provas, se existente.

As melhorias sugeridas na reunião, com o devido consenso, devem ser registradas em ata e encaminhadas ao Gestor de Segurança da Informação e para o Encarregado pelo tratamento de dados pessoais para providências cabíveis.

5.6. Documentação

O incidente deve ser documentado de forma detalhada, incluindo todas as ações implementadas nas etapas anteriores e as lições aprendidas com o caso.

O Grupo de Resposta a Incidentes envolvendo dados pessoais deve documentar o incidente, detalhando as informações obtidas, linha de tempo, atores envolvidos, evidências, conclusões, decisões, autorizações e ações tomadas, inclusive as da reunião de lições aprendidas.

Após a neutralização da ameaça, o Encarregado pelo tratamento de dados pessoais deve elaborar um parecer técnico considerando todas as medidas que foram adotadas, apresentando todas as informações relevantes, tais como, informações sobre o incidente em si (quando foi identificado, qual sua natureza, danos ou potenciais danos causados, a extensão, a relevância e a repercussão desses danos, etc); providências adotadas para preservação das evidências, procedimentos seguidos para a contenção da crise; medidas de correção técnicas e administrativas adotadas; questionamentos e demandas externas (requerimentos de titulares de dados, autoridades e imprensa, bem como suas respostas).

5.7. Comunicação

A ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, deve ser comunicada à Autoridade Nacional de Proteção de Dados – ANPD e ao titular afetado. A depender da situação, as informações a serem prestadas à Autoridade Nacional de Proteção de Dados - ANPD poderá ocorrer por meio de solicitações, comunicações ou auditorias, com a finalidade principal de demonstrar, para o órgão fiscalizador, a adequação (ou intenção de adequação) aos preceitos da Lei Geral de Proteção de Dados Pessoais - LGPD.

Com a máxima brevidade possível, no caso de incidente envolvendo dados pessoais, a situação deve ser encaminhada para análise do Núcleo de Segurança da Informação e Privacidade para avaliar se houve risco ou dano relevante aos titulares dos dados impactados, convocando o Comitê de Segurança da Informação para apreciar a situação, sempre que necessário.

Caso um Incidente seja identificado como relevante e a sua comunicação à ANPD seja determinada a comunicação elaborada deverá conter:

a) A descrição da natureza e da categoria dos dados pessoais afetados (ex. dados sensíveis, dados de criança, dados cadastrais etc.);

b) As informações sobre os titulares dos dados pessoais envolvidos, o número de titulares afetados e o país de residência dos titulares dos dados pessoais afetados;

c) A indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados pessoais, observados os segredos comercial e industrial;

d) Os riscos relacionados ao incidente;

e) Os motivos da demora, no caso de a comunicação não ter sido feita de forma imediata;

f) As medidas que foram e as que serão adotadas para reverter ou mitigar os efeitos do Incidente; e

g) Demais dados solicitados no formulário de comunicação de incidentes disponibilizado pela Autoridade Nacional de Proteção de Dados - ANPD.

Caso seja necessária a comunicação sobre o incidente aos titulares dos dados pessoais afetados, os responsáveis pelos sistemas/processos impactados, irão desenvolver a mensagem da comunicação, priorizando os fatos ocorridos; as medidas já tomadas para minimizar o impacto dos efeitos; as eventuais medidas que possam ser tomadas pelos próprios titulares dos dados pessoais afetados para mitigar riscos; e os canais de contato para sanar dúvidas. Tal comunicado deverá ser submetido ao Encarregado pelo Tratamento de Dados Pessoais para validação e publicado pela Assessoria de Comunicação.

6. INCIDENTES DE SEGURANÇA ENVOLVENDO DADOS PESSOAIS EM MEIO FÍSICO

6.1. Detecção

A identificação de qualquer incidente de segurança é aspecto chave para a boa implementação de um Plano de Respostas

Desta forma, todos devem atentar-se, principalmente, aos sinais mais comuns que podem desencadear um incidente, como perda ou furto de documentos, arquivos, dispositivos, entre outros.

Além disto, a comunicação inicial do incidente pode ser proveniente de qualquer fonte, tais como: e-mails, sistemas, telefone, “Fale Conosco”, Plataforma “Fala.BR”, TI Ajudo.

Portanto, deve haver um trabalho maciço de sensibilização e capacitação de servidores/funcionários/colaboradores, para que, proativamente, esses tenham a capacidade de identificar e informar eventual incidente ou vazamento de dados pessoais, de que tenham conhecimento.

Uma vez detectado um incidente ou detectada a mera suspeita de um incidente, o NOTIFICADOR deverá comunicar imediatamente ao ACIONADOR, preferencialmente por meio do TI AJUDO. Na medida do possível, essa comunicação deverá conter:

a) a hora e a data em que a suspeita do Incidente foi descoberta;

b) o tipo de informações envolvidas;

c) a causa e a extensão do Incidente;

d) o contexto do ocorrido; e

e) qualquer informação adicional que sirva para facilitar o entendimento do evento, suas causas e consequências.

Ao verificar indícios de incidente, orienta-se por preencher o formulário para apoiar a avaliação interna do incidente, com as informações que dispor inicialmente. O preenchimento completo do formulário será realizado em etapas posteriores.

6.2. Triagem

O ACIONADOR deve fazer a avaliação preliminar ou contatar imediatamente outro ACIONADOR em condições de realizar a referida avaliação, descartando as notificações nulas ou claramente improcedentes, tomando os devidos cuidados de registrar os motivos do descarte.

Na avaliação preliminar, devem ser buscadas informações sobre os sistemas que foram possivelmente impactados, sua criticidade, quais os danos aparentes e o risco da situação se agravar se não houver resposta imediata.

Conforme a avaliação preliminar, incidentes que não envolvem sistemas online e que seguramente não apresentam riscos relevantes aos titulares de dados pela falta de ação imediata podem ser reencaminhados para trâmites regulares dos setores pertinentes, mantendo o Protocolo Geral e Arquivo cientes do ocorrido.

Identificada a existência de dados pessoais, o Encarregado pelo Tratamento de Dados Pessoais também deve ser notificado.

Em caso de incidentes que exigem resposta imediata ou melhor avaliação, o Gestor de Segurança da Informação deve ser acionado e passa-se para as fases seguintes.

6.3. Avaliação

Nesta fase deve ser iniciada uma avaliação mais detalhada do incidente, classificando-o e definindo sua criticidade.

A criticidade do incidente pode ser definida de acordo com as seguintes classificações:

a) Alto (Impacto Grave) - Incidente que afeta informações críticas, com potencial para gerar impacto negativo sobre a instituição;

b) Médio (Impacto Significativo) - Incidente que afeta informações não críticas, sem impacto negativo à instituição;

c) Baixo (Impacto Mínimo) - Possível incidente.

Deve-se procurar identificar a causa do incidente, atores e ações envolvidas, vulnerabilidades exploradas, visando determinar ações para as demais fases.

Recomenda-se preencher completamente o formulário para apoiar a avaliação interna do incidente para subsidiar o processo de análise.

Pode ser importante engajar especialistas dos setores afetados para colaborar e isso deve ser feito a qualquer momento que julgar adequado e viável.

Caso os processos envolvidos tenham chefes responsáveis identificados na estrutura organizacional, estes devem ser acionados, para que se manifestem, colaborando nas estratégias de atuação.

6.4. Contenção, Erradicação e Recuperação

O objetivo das medidas de contenção, erradicação e recuperação é limitar o dano e restabelecer a segurança. Como neste fluxo trata-se de incidentes não relacionados a recursos computacionais, mas essencialmente de atividade humana, os procedimentos podem envolver

sindicância administrativa, processo administrativo disciplinar, entre outras medidas dispostas na legislação aplicável ao caso.

O Encarregado pelo tratamento de dados pessoais deve acompanhar os processos para adoção de medidas cabíveis quanto à notificação do incidente aos titulares e àAutoridade Nacional de Proteção de Dados - ANPD, caso necessário.

6.5. Lições aprendidas

Com o incidente contido e sua resolução encaminhada, o Núcleo de Segurança da Informação e Privacidade deverá subsidiar o Comitê de Segurança da Informação para que haja uma reunião onde sejam apresentadas lições aprendidas, com convidados a seu critério, com o objetivo de discutir erros e dificuldades encontradas, propor melhorias para os processos de segurança e de privacidade da informação, avaliar a eficácia deste Plano e subsidiar a documentação da causa-raiz, bem como outras provas.

6.6. Documentação

O Núcleo de Segurança da Informação e Privacidade deverá coordenar a documentação do incidente, de modo que detalhe as informações obtidas, linha de tempo, atores envolvidos, evidências, conclusões, decisões, autorizações e ações tomadas, inclusive as da reunião de lições aprendidas.

6.7. Comunicação

Assim que possível, no caso de incidente envolvendo dados pessoais, a situação deve ser encaminhada para análise para avaliar se houve risco ou dano relevante aos titulares dos dados pessoais impactados.

Caso se conclua que o incidente acarretou risco ou dano relevante aos titulares de dados pessoais, o Encarregado pelo Tratamento de Dados Pessoais deverá coordenar junto a Assessoria de Comunicação e com o Gesto de Segurança da Informação para fazer as comunicações obrigatórias por Lei.

7. REFERÊNCIAS

I - AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/outros-documentosexternos/anpd_guia_agentes_de_tratamento.pdf> Acesso em:05 out. 2022.

II - MINISTÉRIO DA ECONOMIA. Guia de Resposta a Incidentes de Segurança. Disponível em: < file:///D:/Users/marcia.soares/Downloads/guia_resposta_incidentes.pdf> Acesso em:05 out. 2022.

III - BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 05 out. 2022.

MINISTÉRIO DA DEFESA

PROGRAMA DE GESTÃO EM PRIVACIDADE

ANEXO E

PLANO DE COMUNICAÇÃO RELATIVO AO TRATAMENTO DE DADOS PESSOAIS

1. PROPÓSITO

Estabelecer procedimentos internos e formas de disseminação de conhecimento quanto aos aspectos afetos à proteção de dados pessoais, bem como os procedimentos para comunicação com titulares de dados pessoais e com a Autoridade Nacional de Proteção de Dados Pessoais - ANPD.

2. DISSEMINAÇÃO DE CONHECIMENTO

As ações de disseminação de conhecimento têm por objetivo atender aos preceitos da Lei Geral de Proteção de Dados Pessoais - LGPD e contribuir para o incremento da mentalidade de proteção de dados pessoais no âmbito da administração central do Ministério da Defesa.

Para tanto serão estabelecidos repositórios institucionais na internet e intranet para fins específicos.

2.1. Repositório Institucional na Internet

Tem por finalidade cumprir os preceitos da Lei Geral de Proteção de Dados Pessoais - LGPD quanto ao acesso à informação sobre os tratamentos de dados pessoais realizados pelo Ministério da Defesa. Atualmente este repositório está publicado em https://www.gov.br/defesa/pt-br/acesso-a-informacao/lei-geral-de-protecao-de-dados-pessoais-lgpd.

O *checklist* abaixo relaciona as informações que devem ser publicadas e mantidas atualizadas:

a) hipóteses em que, no exercício de suas competências, o Ministério da Defesa realiza o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos (art. 23, inciso I da LGPD)

b) a identidade e as informações de contato do encarregado, de forma clara e objetiva (art. 41 § 1º da LGPD);

c) a forma de requerer os direitos dos titulares de dados pessoais (plataforma Fala.br) (art. 18 § 3º e § 5º da LGPD);

d) atos normativos quanto ao tratamento de dados pessoais (art. 50 da LGPD); e

e) os termos de uso e avisos de privacidade de serviços digitais que tratam dados pessoais (art. 23, inciso I c/c art. 18 da LGPD).

Conforme a Diretriz de Proteção de Dados Pessoais, as unidades finalísticas fornecerão as informações para o Encarregado pelo tratamento de dados pessoais, que as consolidará e encaminhará para a Assessoria Especial de Comunicação Social - ASCOM.

2.2. Repositório Institucional na Intranet

Tem por finalidade disseminar informações e boas práticas sobre proteção de dados pessoais no âmbito da administração central do Ministério da Defesa, por meio **links**, documentos relativos à Lei Geral de Proteção de Dados Pessoais - LGPD, leis, normativos, cartilhas, guias e orientações. O conteúdo deste repositório será produzido sob orientação do Encarregado pelo tratamento de dados pessoais.

3. PROCEDIMENTOS PARA COMUNICAÇÃO

3.1. Orientação quanto ao tratamento de dados pessoais e esclarecimento de dúvidas

O Encarregado pelo tratamento de dados pessoais é o responsável por prestar orientações e esclarecer dúvidas sobre o tratamento de dados pessoais. Todos que efetuam o tratamento de dados pessoais em nome da administração central do Ministério da Defesa podem entrar em contato com o Encarregado por meio dos seguintes canais:

a) Email: encarregado@defesa.gov.br

b) Telefone: 61 2023-xxxx

3.2. Notificação de incidentes envolvendo dados pessoais

Quando da ocorrência de incidente envolvendo dados pessoais, o Encarregado pelo tratamento de dados pessoais deverá ser notificado mediante o registro do incidente na plataforma TI AJUDO.

Tal notificação também pode ser encaminhada ao Encarregado via Super Gov.

3.3. Comunicação com a Autoridade Nacional de Proteção de Dados Pessoais (ANPD):

A comunicação com a Autoridade Nacional de Proteção de Dados - ANPD em caso de incidentes de segurança envolvendo dados pessoais será realizada pelo Encarregado pela Proteção de Dados Pessoais da administração central do Ministério da Defesa, conforme procedimentos

estabelecidos pela Autoridade Nacional de Proteção de Dados - ANPD [18], tendo como base o modelo padronizado no Apêndice "A" do anexo "D" deste Programa de Gestão em Privacidade - PGP.

3.4. Comunicação com Titulares de Dados Pessoais

A comunicação do incidente aos titulares deve ser feita em linguagem clara e simplificada e mencionar, no que couber, os elementos previstos no §1º do art. 48 da Lei Geral de Proteção de Dados Pessoais - LGPD, tais como: a descrição geral do incidente e a data da ocorrência; a natureza dos dados pessoais afetados e os riscos relacionados ao incidente; as medidas tomadas e recomendadas para mitigar os efeitos do incidente; o contato do encarregado ou o ponto de contato para que os titulares obtenham informações a respeito do incidente; outras informações que possam auxiliar os titulares a prevenir possíveis danos. A comunicação deve ser feita de forma individual e diretamente aos titulares, sempre que possível.

4. CANAIS OFICIAIS DE COMUNICAÇÃO

No âmbito do Setor Público, os canais de contato abaixo poderão ser empregados no processo de comunicação de incidentes pelas autoridades competentes. Observa-se, entretanto, que cada um dos órgãos listados possui atribuições legais e regimentais distintas, e que a Autoridade Nacional de Proteção de Dados - ANPD é o ponto focal para a Lei Geral de Proteção de Dados Pessoais - LGPD e a autoridade administrativa fiscalizatória para recebimento de incidentes envolvendo dados pessoais:

a) Autoridade Nacional de Proteção de Dados - ANPD: formulário de comunicação de incidentes. A comunicação deverá ser formalizada pelo Encarregado pelo tratamento de dados pessoais;

b) Coordenação-Geral de Segurança da Informação (CGSIN/SGD/SEDGG/ME): e-mail para cgsin@economia.gov.br. A comunicação deve ser realizada pela Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR ou pelo Gestor de Segurança da Informação;

c) CTIR Gov: e-mail para ctir@ctir.gov.br. A comunicação deve ser realizada pela Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR ou pelo Gestor de Segurança da Informação, seguindo os padrões de notificação de incidentes de segurança do Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo - CTIR-GOV;

d) Encarregado pelo tratamento de dados pessoais da administração central do Ministério da Defesa: encarregado@defesa.gov.br, TI Ajudo e tel: 2023-5356;

e) Gestor de Segurança da Informação: gestor_seginfo@defesa.gov.br

f) Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR - ACMD: abuse@defesa.gov.br.

[18] https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca

MINISTÉRIO DA DEFESA

PROGRAMA DE GESTÃO EM PRIVACIDADE

ANEXO F

TRILHAS DE CONHECIMENTO NA ÁREA DE PROTEÇÃO DE DADOS PESSOAIS

As trilhas de conhecimento abaixo relacionadas agregam informações sobre eventos de capacitação que podem ser realizados no âmbito da administração central do MD de modo a elevar a maturidade em proteção de dados pessoais.

a) Trilha de conhecimento 1:

Público Alvo: Servidores (civis e militares) e colaboradores que exercem atividade profissional envolvendo, direta ou indiretamente, o tratamento de dados pessoais.

Curso	Órgão	Carga horária	Modalidade	Custo	Periodicidade de oferta
Curso de Tratamento e Proteção de Dados Pessoais https://ead.defesa.gov.br/course/view.php?id=8	MD	10 h/a	EAD	Gratuito	Mensal

b) Trilha de conhecimento 2:

Público Alvo: Servidores (civis e militares) e colaboradores que exercem atividade profissional envolvendo diretamente o tratamento de dados pessoais.

Curso	Órgão	Carga horária	Modalidade	Custo	Periodicidade de oferta
Fundamentos da Lei Geral de Proteção de Dados Pessoais https://www.escolavirtual.gov.br/curso/603	EvG/ENAP	10 h/a	EAD	Gratuito	Mensal
Proteção de Dados Pessoais no Setor Público https://www.escolavirtual.gov.br/curso/290	EvG/ENAP	10 h/a	EAD	Gratuito	Mensal

c) Trilha de conhecimento 3:

Público Alvo: Servidores (civis e militares) e colaboradores que exercem atividade profissional no setor de recursos humanos, protocolo, transparência e outros que tratam grande volume de dados pessoais.

Curso	Órgão	Carga horária	Modalidade	Custo	Periodicidade de oferta

Governança de Dados https://www.escolavirtual.gov.br/curso/270	EvG/ENAP	30 h/a	EAD	Gratuito	Mensal
Governança de Dados na Transformação Digital https://www.escolavirtual.gov.br/curso/536	EvG/ENAP	17 h/a	EAD	Gratuito	Mensal

d) Trilha de conhecimento 4:

Público Alvo: Servidores (civis e militares) e colaboradores responsáveis por coordenar a implementação da Diretriz de Proteção de Dados Pessoais nas unidades finalísticas ou que atuem auxiliando o Encarregado pelo tratamento de dados pessoais.

Curso	Órgão	Carga horária	Modalidade	Custo	Periodicidade de oferta
LGPD na prática https://esr.rnp.br/cursos/lgpd-na-pratica-ead-gti46/	ESR/RNP	40 h/a	EAD	Pago	Anual

e) Trilha de conhecimento 5:

Público Alvo: Servidor (civis e militares) que desempenha o encargo de Encarregado pelo tratamento de dados pessoais.

Curso	Órgão	Carga horária	Modalidade	Custo	Periodicidade de oferta
Atuação do Encarregado na proteção de dados: a função de orientar https://suap.enap.gov.br/portaldoaluno/curso/1798/?area=2	EvG/ENAP	15 h/a	Remoto	Gratuito	Conforme calendário da ENAP
EXIN ISFS - Information Security Foundation ISO/IEC 27001 https://esr.rnp.br/cursos/oficial-exin-isfs-information-security-foundation-iso-iec-27001-ead-parceria-oficial-exin-gti48/	ESR/RNP	16 h/a	EAD	Pago	Anual
EXIN PDPE - Privacy & Data Protection Essentials EAD https://esr.rnp.br/cursos/oficial-exin-pdpe-privacy-data-protection-essentials-ead-parceria-oficial-exin-gti50/	ESR/RNP	16 h/a	EAD	Pago	Anual

EXIN PDPF - Privacy & Data Protection Foudation EAD https://esr.rnp.br/cursos/oficial-exin-pdpf-privacy-data-protection-foudation-ead-parceria-oficial-exin-gti51/	ESR/RNP	16 h/a	EAD	Pago	Anual
EXIN PDPP - Privacy and Data Protection Practitioner https://esr.rnp.br/cursos/oficial-exin-pdpp-privacy-and-data-protection-practitioner-ead-parceria-oficial-exin-gti52/	ESR/RNP	24 h/a	EAD	Pago	Anual

f) Trilha de conhecimento 6:

Público Alvo: Servidores (civis e militares) e colaboradores que atuam na área de Tecnologia da Informação.

Curso	Órgão	Carga horária	Modalidade	Custo	Periodicidade de oferta
Gestão de Riscos de Segurança da Informação e Privacidade https://esr.rnp.br/cursos/gestao-de-riscos-de-seguranca-da-informacao-e-privacidade-ead-gti36/	ESR/RNP	40 h/a	EAD	Pago	Anual