Assessoria de Controle Interno (ACI)

PROGRAMA DE GESTÃO EM PRIVACIDADE DO HFA

1ª Edição
Brasília/DF – 2023

SUMÁRIO

1 INTRODUÇÃO

A Lei Geral de Proteção de Dados Pessoais – LGPD (Lei n° 13.709, de 14 e agosto de 2018) foi promulgada para proteger os direitos fundamentais de liberdade, de privacidade e a livre formação da personalidade de cada indivíduo. Essa Lei versa sobre o tratamento de dados pessoais, dispostos em meio físico ou digital, feito por pessoa física ou jurídica de direito público ou privado e engloba um amplo conjunto de operações efetuadas em meios manuais ou digitais.

A adequação do Hospital das Forças Armadas - HFA em relação à LGPD envolve uma transformação cultural que deve alcançar os níveis estratégico, tático e operacional da instituição. Essa transformação envolve: considerar a privacidade dos dados pessoais do cidadão desde a fase de concepção do serviço ou produto até sua execução (Privacidade by Design); e promover ações de conscientização de todo corpo funcional no sentido de incorporar o respeito à privacidade dos dados pessoais nas atividades institucionais cotidianas.

Desta forma, este Programa de Gestão em Privacidade - PGP visa direcionar a adequação do HFA a LGPD, buscando capturar e consolidar os requisitos de privacidade com o intuito de ditar e influenciar como os dados pessoais são manuseados na totalidade do seu ciclo de vida, dentro deste nosocômio. Baseando esse trabalho nos princípios da LGPD, conforme listados na figura abaixo:

Figura 1. Princípios da LGPD

O presente documento apresenta o Programa de Gestão em Privacidade a ser implementado no HFA que estará sujeito a atualização conforme as diretrizes emanadas pela Autoridade Nacional de Dados Pessoais (ANPD).

2 OBJETIVO

Estabelecer as medidas necessárias para a proteção de dados pessoais tratados no âmbito do HFA e promover um ciclo de melhoria contínua para cumprir a legislações pertinentes. Protegendo os dados desde a fase inicial de coleta e durante todo o seu ciclo de vida, até sua eliminação. Assim como, a criação de uma cultura de segurança e privacidade dos dados pessoais nos diversos setores do hospital através da capacitação de pessoal e a utilização de ferramentas de comunicação e difusão.

3 ETAPAS

Segundo a Diretriz para Proteção de Dados Pessoais do Ministério da Defesa – MD, o Programa de Gestão em Privacidade-PGP é um ciclo contínuo divido em três fases (figura 2) com foco na mitigação dos riscos inerentes. Devendo ser aprimorado constantemente mediante o emprego de um ciclo PDCA (*Plan*, *Do*, *Check* e *Act*), permitindo seu aperfeiçoamento e adequação à evolução do tema.

Figura 2. Etapas do PGP

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;

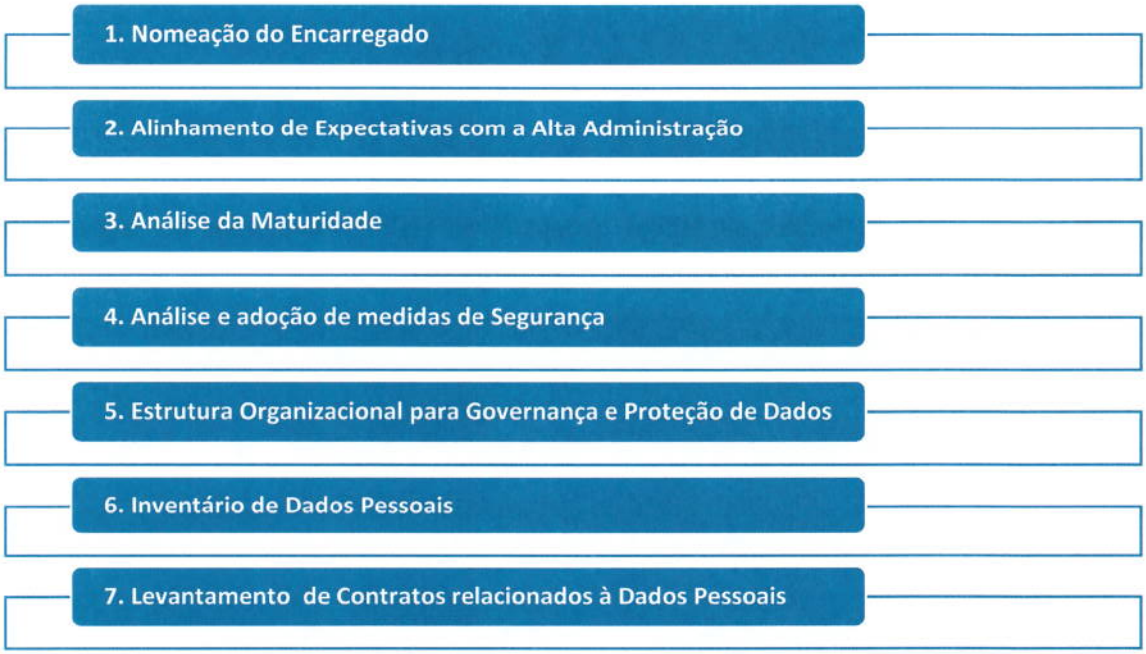
d) fazer cumprir, no âmbito de suas atribuições e competências, a Política de Segurança da Informação;

e) determinar, no âmbito de suas atribuições e competências, que terceiros contratados estejam em conformidade com a LGPD; e

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

3.1 ETAPA 1 - INICIAÇÃO E PLANEJAMENTO

Esta etapa busca compreender quais são as primeiras informações e os dados que devem ser conhecidos. Assim, ela é constituída pelos marcos apresentados abaixo, que serão detalhados logo a seguir.



3.1.1 NOMEAÇÃO DO ENCARREGADO

O Encarregado pelo tratamento de dados pessoais é a 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 (inciso VIII, art. 5º da LGPD). De acordo com § 2º do art. 41 da Lei Geral de Proteção de Dados Pessoais, são atribuições do Encarregado, as seguintes atividades:

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

b) Receber comunicações da ANPD 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) Apoiar a definição das diretrizes de construção do inventário de dados pessoais relativas ao registro das operações de tratamento de dados pessoais determinado pelo art. 37 da LGPD;

e) Conduzir ou aconselhar a elaboração de relatório de impacto à proteção de dados pessoais, de acordo com casos previstos pela LGPD, em que tal documento é necessário;

f) Conduzir ou aconselhar a implementação de regras de boas práticas e de governança especificadas pelo art. 50 da LGPD; e

g) Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

O Encarregado de dados do HFA, foi designado conforme Portaria SG-MD Nº 1.417, de 18 de março de 2022, publicado no Boletim Interno n° 054/HFA, de 21 de março de 2022. Os dados do Encarregado estão públicos e acessíveis no sítio eletrônico da internet do HFA, pelo link https://www.gov.br/hfa/pt-br/acesso-a-informacao/encarregado-pelo-tratamento-de-dados-pessoais-dpo.

3.1.2 ALINHAMENTO DE EXPECTATIVAS COM A ALTA ADMINISTRAÇÃO

Nesta etapa são definidos os atores previstos na LGPD, envolvidos no tratamento dos dados pessoais e quais suas responsabilidades neste processo:

TITULAR	No papel central, por sua importância, tem-se o titular, que é qualquer pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
CONTROLADOR	Pessoa natural ou jurídica, de direito público ou privado, a quem competem às decisões referentes ao tratamento de dados pessoais.
OPERADOR	Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.
AGENTES DE TRATAMENTO	O controlador e o operador
ENCARREGADO	Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD;
AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD)	Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional.

Tabela 1. Atores da LGPD

O titular de dados pessoais, no âmbito do HFA é prioritariamente o paciente atendido no hospital, e eventualmente, os servidores do HFA que tenham seus dados tratados por algum setor administrativo do hospital.

O Controlador, conforme a LGPD, é a pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais. Desta forma, é a autoridade responsável pelas decisões administrativas do órgão/instituição. Podendo a autoridade delegar a função de controlador a outro membro da alta administração do órgão. O controlador é crucial para a efetividade das ações relacionadas ao cumprimento das obrigações estipuladas pela LGPD.

A função de Operador se caracteriza por ser pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. No HFA, se configuram como operadores, todas as divisões/setores ou empresa terceirizada que realize o tratamento de dados pessoais, através da coleta, processamento e armazenamento de dados. Seja o processo realizado em meio digital ou físico.

3.1.3 ANÁLISE DA MATURIDADE - DIAGNÓSTICO DO ATUAL ESTÁGIO DE ADEQUAÇÃO À LGPD

Segundo as orientações Secretaria de Governo Digital – SGD, será realizado periodicamente uma avaliação da maturidade do HFA em relação à segurança e proteção de dados e sua adequação a LGPD. O resultado dessa avaliação alimentará a fase de planejamento do ciclo de gestão do PGP.

3.1.4 ANÁLISE E ADOÇÃO DE MEDIDAS DE SEGURANÇA, DIRETRIZES E CULTURA INTERNA

Deve ser adotado o conceito de privacidade desde a concepção dos serviços ou atividades desenvolvidas no órgão (do inglês Privacy by Design), visando uma maior segurança e proteção dos dados pessoais tratados em cada processo desenvolvido nas divisões e setores do HFA que trabalham com coleta, processamento e armazenamento de dados pessoais de pacientes ou servidores do hospital, conforme previsto no § 2º, artigo 46 da LGPD. Tal segurança na privacidade pode ser alcançada por meio da aplicação dos 7 (sete) Princípios Fundamentais (Cavoukian, 2009), que são os seguintes:

a) Proativo, e não reativo; preventivo, e não corretivo;
b) Privacidade deve ser o padrão dos sistemas de TI ou práticas de negócio;
c) Privacidade incorporada ao projeto (design);
d) Funcionalidade total;
e) Segurança e proteção de ponta a ponta durante o ciclo de vida de tratamento dos dados;

f) Visibilidade e Transparência; e
g) Respeito pela privacidade do usuário.

Segundo o previsto pelo caput do art. 46 da LGPD, a proteção dos dados pessoais é alcançada por meio de medidas de segurança, técnicas e administrativas.

> *"Art. 46. 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"*

Assim, os agentes de tratamento ou qualquer outra pessoa que participe das fases do ciclo de vida do tratamento de dados pessoais são obrigados a assegurar a segurança da informação para proteção dos dados pessoais.

Desta forma, as ações realizadas e as documentações produzidas para adequação à LGPD, tais como o presente PGP, o IDP, os Termos de Política de Uso e Privacidade, o Levantamento dos Riscos de Segurança e Privacidade, a adequação dos Contratos, o Relatório de Impacto de Proteção dos Dados, o Plano de Resposta a Incidentes, bem como documentos internos, entre outros, serão construídas tendo por base o conceito de Privacy by Design.

3.1.5 ESTRUTURA ORGANIZACIONAL PARA A GOVERNANÇA E PROTEÇÃO DE DADOS

A Governança e a proteção dos Dados caberão ao Comitê de Governança Digital, Privacidade e Segurança da Informação - CGDPSI, criado por meio da Instrução Normativa Nº 11 /CMT LOG-HFA de 25 de Julho de 2023, sendo composto pelos seguintes integrantes: o programa de gestão em privacidade é ciclo contínuo divido em três fases (figura 2) Coordenador-Geral do Hospital das Forças Armadas (Presidente);

a) Subdiretor Técnico de Saúde;
b) Subdiretor Técnico de Ensino e Pesquisa;
c) Chefes das Divisões e Assessorias do Comando Logístico; e
d) Demais chefias e servidores convocados de acordo com a pauta a ser discutida.

O Comitê tem entre suas atribuições, tratar de assuntos relativos à Proteção de Dados Pessoais e Privacidade. Dentro deste, destaca-se a atividade de assessorar a implementação das ações de Proteção de Dados Pessoais; avaliar os mecanismos de tratamento e proteção dos dados existentes e propor políticas, estratégias e metas para a conformidade do HFA com as disposições da legislação afim; e auxiliar o controlador de dados, quando solicitado, na formulação de princípios e diretrizes para a gestão de dados pessoais e na sua regulamentação.

O Comitê deverá balizar os seus trabalhos pela Política de Segurança da Informação e Comunicações – PoSIC/HFA, através da Orientação Normativa Nº 05/CMT LOG HFA, de 15 de agosto de 2019. Que trata do uso e compartilhamento do conteúdo de dados, informações e documentos no âmbito do HFA, em todo o seu ciclo de vida – criação, manuseio, divulgação, armazenamento, transporte e descarte, visando, normas e procedimentos pertinentes, requisitos regulamentares e contratuais, valores éticos e as melhores práticas de segurança da informação e comunicações.

3.1.6 INVENTÁRIO DE DADOS PESSOAIS (IDP)

Visando mapear os dados pessoais e fazer um balanço do que o HFA faz com esses dados, identificando quais são os dados, onde estão e que operações são realizadas com eles (LGPD, art. 5º, VI), será empregada a planilha de Inventário de Dados Pessoais (ANEXO A), conforme o modelo da disponibilizado pela Secretaria de Governo Digital – SGD, que tem como base as metodologias adotadas pela ANPD e também por várias agências estrangeiras de tratamento de dados pessoais.

Assim, para obter um mapeamento dos setores e processos que trabalham com dados pessoais no HFA e também verificar se são dados sensíveis. Será realizado o preenchimento da planilha do Inventário de Dados Pessoais nos diversos setores do hospital.

O inventário consiste em uma planilha eletrônica que deve ser preenchida pelos setores do hospital, e buscam o preenchimento das seguintes informações:

a) Agentes de tratamento;
b) Finalidade (o que a instituição faz com o dado pessoal);
c) Hipótese para realização do tratamento (art. 7° e 11 da LGPD);
d) Previsão legal;
e) Dados pessoais tratados pela instituição;
f) Categoria dos titulares dos dados;
g) Tempo de retenção;
h) Instituições com as quais os dados são compartilhados;
i) Transferência internacional (art. 33 da LGPD); e
j) Medidas de segurança.

O inventário de dados pessoais é um importante documento de governança, fornecendo subsídios para avaliação de impacto à proteção de dados pessoais, com vistas a verificar a conformidade da instituição à LGPD, pois permite identificar os principais setores envolvidos no tratamento de dados sensíveis.

3.1.7 LEVANTAMENTO DOS CONTRATOS RELACIONADOS À DADOS PESSOAIS

O levantamento feito pelo Inventário de Dados Pessoais dos serviços que tratam dados pessoais viabiliza a realização de um cruzamento com os contratos que os suportam. Esse mapeamento dos contratos relativos ao tratamento de dados pessoais contribui para possíveis e necessárias adequações contratuais, tanto nos contratos existentes, quanto aos futuros contratos.

Desta forma, serão verificados os seguintes tópicos dos contratos existentes entre o HFA e as empresas terceirizadas prestadoras de serviços, para a devida necessidade de adequação dos mesmos a LGPD:

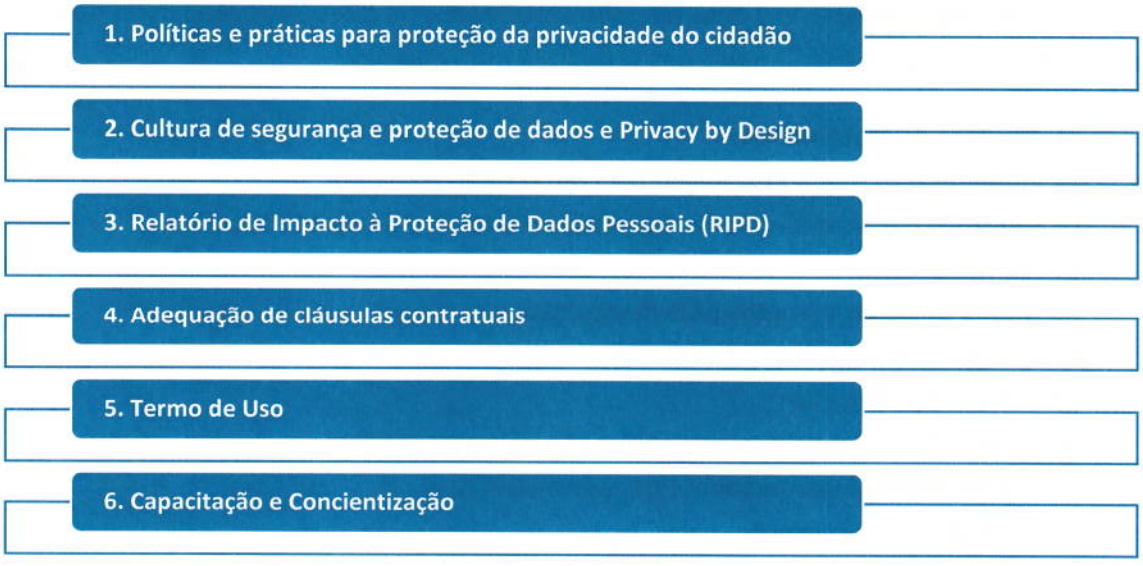
a) Correlação dos serviços/processos de negócio com os contratos que os suportam;

b) Mapeamento dos contratos que coletam, transferem e processam dados pessoais; e

c) Possíveis e necessárias adequações contratuais, tanto nos existentes, quanto nos futuros.

3.2 ETAPA 2 - CONSTRUÇÃO E EXECUÇÃO

Nesta etapa de construção e execução serão implementados e detalhados os seguintes marcos:



3.2.1 POLÍTICAS E PRÁTICAS PARA PROTEÇÃO DA PRIVACIDADE DO CIDADÃO

A LGPD em seu art. 7º dispõe sobre as hipóteses de tratamento dos dados pessoais, e no seu art. 11 sobre as hipóteses de tratamento para os dados pessoais sensíveis, que visão verificar se controlador ou operador tem permissão de tratar os dados, conforme a LGPD. As hipóteses de tratamento estão dispostas no quadro abaixo:

HIPÓTESE DE TRATAMENTO	DISPOSITIVO LEGAL PARA O TRATAMENTO DE DADOS PESSOAIS	DISPOSITIVO LEGAL PARA O TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS
Hipótese 1: Mediante consentimento do titular	LGPD, art. 7º, I	LGPD, art. 11, I
Hipótese 2: Para o cumprimento de obrigação legal ou regulatória	LGPD, art. 7º, II	LGPD, art. 11, II, "a"
Hipótese 3: Para a execução de políticas públicas	LGPD, art. 7º, inciso III	LGPD, art. 11, II, "b"
Hipótese 4: Para a realização de estudos e pesquisas	LGPD, art. 7º, inciso IV	LGPD, art. 11, II, "c"
Hipótese 5: Para a execução ou preparação de contrato	LGPD, art. 7º, inciso V	Não se aplica
Hipótese 6: Para o exercício de direitos em processo judicial, administrativo ou arbitral	LGPD, art. 7º, inciso VI	LGPD, art. 11, II, "d"
Hipótese 7: Para a proteção da vida ou da incolumidade física do titular ou de terceiro	LGPD, art. 7º, inciso VII	LGPD, art. 11, II, "e"
Hipótese 8: Para a tutela da saúde do titular	LGPD, art. 7º, inciso VIII	LGPD, art. 11, II, "f"
Hipótese 9: Para atender interesses legítimos do controlador ou de terceiro	LGPD, art. 7º, inciso IX	Não se aplica
Hipótese 10: Para proteção do crédito	LGPD, art. 7º, inciso X	Não se aplica
Hipótese 11: Para a garantia da prevenção à fraude e à segurança do titular	Não se aplica	LGPD, art. 11, II, "g"

Tabela 2. Hipóteses de tratamento de dados pessoais

Considerando o ciclo de vida do tratamento dos dados pessoais (figura 3) e a natureza da atividade fim do HFA ser prestação do serviço médico aos convênios com os fundos de saúde das três forças armadas e com o Ministério da Defesa, a hipóteses de tratamento predominante é a de número 8, que aborda o tratamento dos dados para a tutela da saúde do titular.

Figura 3. Ciclo de vida do tratamento de dados pessoais.

Mas, verificasse também o uso da hipótese de tratamento de número 4, nos setores do hospital onde são realizadas pesquisas médicas, como ocorre na Direção Técnica de Ensino e Pesquisa (DTEP), nesses casos, para atender a LGPD, existe a necessidade da autorização do participante para o uso de seus dados pessoais nas pesquisas desenvolvidas.

Outra hipótese de tratamento de dados que deve ser aplicado no hospital é a de número 9, que visa atender ao interesse legítimo do controlador. Verificasse a necessidade de sua aplicação nos setores administrativos de controle de pessoal e segurança das instalações. Onde é realizada a escrituração dos apontamentos dos servidores civis e militares do HFA, como feito na Divisão de Recursos Humano (DRH). E também aplicado ao controle da segurança dos estacionamentos internos, realizado pela Assessoria de Segurança (A Seg).

Em consequência, as ações decorrentes do PGP devem estar relacionadas ao Plano de Integridade e podem ser utilizadas como práticas de 2ª Linha de controle interno.

Serão realizadas as seguintes atividades na implantação da LGPD no HFA, visando atingir o objetivo deste programa e facilitar a execução de uma governança em privacidade.

Nº	ATIVIDADES A EMPREENDER	COORDENAÇÃO
1	Designação do Encarregado pelo Tratamento de Dados Pessoais e seus dados de contato no sítio institucional do HFA	Comandante Logístico
2	Implementar a estrutura de proteção de dados pessoais	Comitê de Governança Digital
3	Instituir o Programa de Gestão em Privacidade - PGP	
4	Comunicar internamente os objetivos do PGP	
5	Estabelecer um plano de comunicação no âmbito do PGP	
6	Estabelecer e acompanhar indicadores no âmbito PGP	
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	
8	Alocar recursos para a implementação de mecanismos para tratamento de dados pessoais	
9	Propor o mapeamento do tratamento de dados nos diversos setores do HFA	Encarregado pelo tratamento de dados pessoais
10	Identificação dos setores do hospital que tratam dados pessoais	
11	Acompanhar e prestar assistência aos trabalhos de tratamento e segurança de dados pessoais, desenvolvidos nos setores que tratam dados pessoais do HFA	
12	Acompanhar a implementação de mecanismos para atender os direitos dos titulares de dados pessoais nos setores de tratamento de dados	
13	Propor atividades para a difusão da cultura de proteção dos dados pessoais dentro do HFA	
14	Prover um canal para recebimento de denúncias e de alertas de ocorrência de irregularidades	
15	Propor atividades para capacitação de pessoal, em cursos relacionados ao tratamento e proteção de dados pessoais	
16	Identificar operadores que realizam tratamento de dados pessoais em nome do HFA.	
17	Propor e acompanhar a adequação dos contratos de serviços de banco de dados prestados por empresas terceirizadas	

Nº	ATIVIDADES A EMPREENDER	COORDENAÇÃO
18	Elaborar plano de resposta a incidentes relacionados ao tratamento de dados pessoais	
19	Elaborar plano de comunicação	
20	Avaliar se os dados pessoais são retidos apenas pelo tempo necessário para cumprir a finalidade do tratamento	
21	Implementar sistema de gestão de consentimentos e exercício dos direitos dos titulares	
22	Atualizar a Política de Segurança da Informação	DTI
23	Atualizar a Política de Classificação da Informação, incluindo a classificação de dados pessoais	
24	Verificar se os sistemas informatizados de banco de dados do HFA e das empresas terceirizadas que prestam serviços, atendem aos requisitos de segurança e disponibilização de dados previstos na LGPD	
25	Revisar e adequar contratos e outros instrumentos que prevejam o tratamento de dados pessoais ao previsto na LGPD	DCAF/Seção de contratos
26	Realizar mapeamento e inventário de dados pessoais	Setores que são agentes de tratamento de dados pessoais
27	Identificar e documentar as finalidades e as bases legais das atividades de tratamento de dados pessoais	
28	Avaliar se a coleta de dados é a estritamente necessária para a finalidade identificada	
29	Identificar processos de negócio e responsáveis que realizam o tratamento de dados pessoais	
30	Implementar mecanismos para atender os direitos dos titulares de dados pessoais	
31	Identificar os dados pessoais compartilhados com terceiros	
32	Registrar eventos relacionados à transferência de dados pessoais compartilhados com terceiros	
33	Classificar os dados tratados em dados pessoais e dados pessoais sensíveis	
34	Monitorar vulnerabilidades técnicas nos sistemas e serviços que tratam dados pessoais, a fim de adequá-los às normas atinentes ao tema	
35	Gerar evidências para comprovar que tomou medidas de segurança técnicas e administrativas para proteger os dados pessoais	
36	Realizar gestão de incidentes para tratar possíveis violações dos dados pessoais	
37	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, quando necessários	
38	Monitorar proativamente a ocorrência de eventos que podem ser associados à violação de dados pessoais	
39	Implementar processo formal para registro, cancelamento e provisionamento de usuários em sistemas que realizam o tratamento de dados pessoais	
40	Manter rastreabilidade dos dados pessoais em meio físico e digital	
41	Elaborar Relatório de Impacto à Proteção de Dados Pessoais (RIPD)	
42	Implementar controles de segurança para riscos identificados no Relatório de Impacto à Proteção de Dados Pessoais (RIPD)	
43	Planejar medidas de segurança desde a fase de concepção do serviço ou produto que irá tratar dados pessoais	
44	Promover a manutenção de sistemas e serviços que tratam dados pessoais, a fim de adequá-los às normas atinentes ao tema	

Tabela 3. Ações prioritárias a empreender

3.2.2 CULTURA DE SEGURANÇA E PROTEÇÃO DE DADOS DESDE O PLANEJAMENTO

A cultura de segurança e proteção dos dados tem como base o conceito de Privacidade desde a Concepção (Privacy by Design), ou seja, a privacidade e a proteção de dados devem ser consideradas desde a concepção e durante todo o ciclo de vida do projeto, sistema, serviço, produto ou processo, segundo a aplicação dos 7 (sete) Princípios Fundamentais (Cavoukian, Ann 2009):

a. Proativo, e não reativo, preventivo, e não corretivo;
b. Privacidade deve ser o padrão dos sistemas de TI ou práticas de negócio;
c. Privacidade incorporada ao projeto (design);
d. Funcionalidade total;
e. Segurança e proteção de ponta a ponta durante o ciclo de vida de tratamento dos dados;
f. Visibilidade e Transparência; e
g. Respeito pela privacidade do usuário.

São agentes de tratamento de dados pessoais os setores do HFA que realizam qualquer fase do ciclo de vida do uso de dados pessoais. Esses setores são responsáveis em assegurar à segurança das informações e também a capacitação dos seus servidores as normas previstas na LGPD. A relação dos setores que são agentes de tratamento de dados no HFA será publicada em Boletim Interno, e atualizada sempre que necessário.

Os agentes de tratamento devem buscar limitar a quantidade de dados pessoais coletados, extensão do tratamento, período de armazenamento e acessibilidade ao mínimo necessário para a concretização da finalidade do tratamento dos dados pessoais. Desta forma, ao contrário do usual, quanto menos dados armazenados, melhor será para a proteção e privacidade.

Além da adoção do conceito e dos princípios, devem ser consideradas medidas de segurança e de contingência para proteger os dados de acessos não autorizados e de situações acidentais, ilícitas ou de qualquer forma de tratamento inadequado, como previsto no art. 46 da LGPD.

3.2.3 RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS (RIPD)

O Relatório de Impacto à Proteção dos Dados Pessoais – RIPD (ANEXO B) representa um instrumento importante de verificação e demonstração da conformidade do tratamento de dados pessoais realizado pela instituição e serve tanto para a análise quanto para a documentação do tratamento dos dados pessoais. O 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.

A elaboração contempla as seguintes etapas.

Figura 4. Atividades do RIPD

O Relatório de Impacto será atualizado quando:

a) Uma tecnologia, serviço ou outra nova iniciativa em que dados pessoais e dados pessoais sensíveis sejam ou devam ser tratados;

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

c) 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);

d) 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);

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

f) 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);

g) 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);

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

i) 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; e

j) Reformas administrativas que implicam em nova estrutura organizacional resultante da incorporação, fusão ou cisão de órgãos, ou entidades.

Assim, atendendo ao recomendado no guia de boas práticas da SGD, será feito a elaboração do RIPD pela Direção Técnica de Saúde (DTS), a Direção Técnica de Ensino e Pesquisa (DTEP) e a Divisão de Recursos Humanos (DRH). Após a confecção do RIPD o mesmo deve ser apreciado pelo Encarregado de dados e posterior aprovação do Controlador do HFA.

3.2.4 ADEQUAÇÃO DE CLÁUSULAS CONTRATUAIS

A seção de contratos, sob a supervisão do Encarregado de dados, deverá realizar a revisão do contrato do serviço de Prontuário Eletrônico de Paciente – PEP, e de outras ferramentas do Sistema de Gestão Hospitalar - SGH/MV, que prestam o serviço de gerenciamento do Banco de Dados dos prontuários dos pacientes atendidos no HFA, bem como os demais contratos do hospital com o objetivo de identificar quais serviços demandam tratamento de dados pessoais, tornando-se necessário a devida adequação aos preceitos previstos pelo artigo 6º e artigo 26 da LGPD:

a. Delimitações claras e objetivas das responsabilidades do controlador e operador;
b. A forma que é realizada a coleta e o tratamento de dados;
c. A existência da possibilidade de o titular acessar os seus dados coletados;
d. A forma que é realizada a correção, bloqueio ou eliminação de dados mediante solicitação do titular;
e. A existência da possibilidade de revogação do consentimento dado pelo titular;
f. O detalhamento de quem tem acesso aos dados, o responsável por seu uso e tratamento, a forma de armazenamento e as particularidades de possíveis auditorias; e
g. As medidas de proteção e segurança dos dados coletados e armazenados pela contratada.

3.2.5 TERMO DE USO E AVISO DE PRIVACIDADE

O Termo de Uso é uma espécie de contrato de adesão cujas cláusulas são estabelecidas de forma unilateral pelo fornecedor do serviço sem que o usuário possa discutir ou modificar substancialmente seu conteúdo. Esse contrato é celebrado entre o prestador e o usuário do serviço e estabelece os direitos e obrigações de cada uma das partes. Cabe destacar, também, que o Aviso de Privacidade faz parte do Termo de Uso e consiste na prestação de informações ao titular sobre o tratamento dos dados pessoais e a privacidade fornecida.

Desta forma, o Termo de Uso devem ser constantemente atualizados a fim de refletir, de modo claro e preciso, as regras aplicáveis ao serviço e as finalidades de coleta, uso, armazenamento, tratamento e proteção dos dados pessoais dos titulares. Devendo o Termo possuir os seguintes tópicos:

a) Aceitação dos Termos e Políticas;
b) Definições;
c) Arcabouço Legal;
d) Descrição do serviço;
e) Direitos do usuário;
f) Responsabilidades do usuário e da Administração Pública;
g) Mudanças no Termo de Uso;
h) Informações para contato; e
i) Foro.

Cumprindo ao previsto na LGPD, deverá ser confeccionada o Aviso de Privacidade e/ou o Termo de Uso, conforme a necessidade e especificidade de cada serviço abaixo listado. O documento será elaborado pelo setor/divisão responsável pelo serviço e com supervisão do Encarregado de dados, conforme o modelo disponibilizado neste Programa (ANEXO C):

a) Serviço de abertura e atualização de prontuário presencial na Divisão de Arquivo Médico e Estatística (DAME), da Direção Técnica de Saúde (DTS);
b) Serviço de acesso a resultado de exames laboratoriais na página internet do HFA, vinculada a Subdivisão de Laboratório de Análises Clínicas (SDLAC)/DTS;
c) Serviço de pesquisas médicas na Divisão de Pesquisa (Div Pesq) da Direção Técnica de Ensino e Pesquisa (DTEP); e
d) Serviço de cursos e capacitação prestados na Divisão de Ensino (Div Ens) da DTEP.

Caberá ao Encarregado de dados indicar/despachar com Controlador do HFA, outros serviços e atividades do HFA, não listados acima, que necessitem também implantar o aviso de privacidade e o Termo de uso.

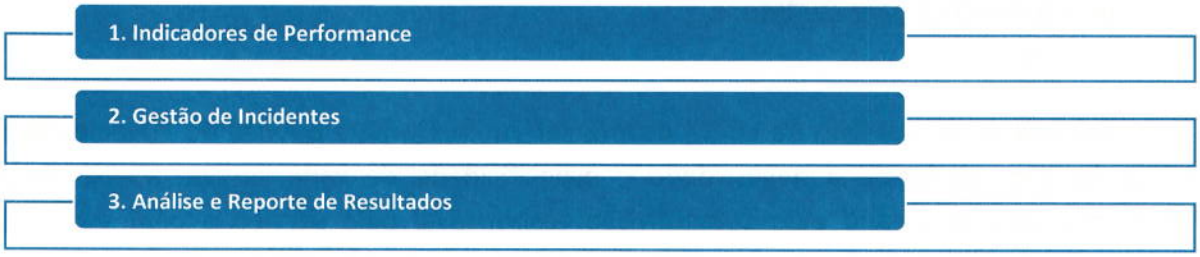
3.2.6 CAPACITAÇÃO E CONSCIENTIZAÇÃO

A capacitação na Lei Geral de Proteção de Dados Pessoais – LGPD será realizada através de cursos online na plataforma digital ou presencial, sendo monitorada a execução pelo Encarregado de dados e sobre a responsabilidade do Chefe dos Setores agentes no tratamento de dados pessoais.

Visando a conscientização organizacional deverá ser disponibilizadas mensagens sobre a LGPD em pop-up no portal eletrônico da intranet do HFA, essa atividade de divulgação será realizada com o apoio da Assessoria de Comunicação do HFA.

3.3 ETAPA 3 – MONITORAMENTO

O Monitoramento é uma atividade contínua e necessária para acompanhar a conformidade do órgão à LGPD. Assim sendo, esta etapa do PGP caberá ao Chefe dos Setores Agentes no tratamento de dados pessoais e ao Encarregado de dados do HFA. Através da coleta e análise de informações, bem como elaboração de relatórios e apresentações de resultados, visando o aprimoramento contínuo do Programa, com os seguintes marcos abaixo identificados:



3.3.1 INDICADORES DE PERFORMANCE

Inicialmente os indicadores de performance do HFA serão os listados abaixo, e serão acompanhados no Plano Anual de Controle Interno (PACI):

1. Resultados do diagnóstico de Adequação à LGPD:

Indicador	Descrição	Fórmula de Cálculo
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: 2022: Inicial

2. Índice de conscientização em segurança de dados:

Indicador	Descrição	Fórmula de Cálculo
Índice de conscientização em segurança de dados	Acompanhar as ações de capacitação e campanhas de fomento à mentalidade de privacidade. Medição: anual	Quantidade de treinamentos realizados/quantidade de treinamentos previstos * 100

3. Índice de serviços com dados pessoais inventariados:

Indicador	Descrição	Fórmula de Cálculo
Índice de operações de tratamento com dados pessoais inventariados	Acompanhar o processo de inventário das operações de tratamento de dados pessoais. Medição: anual	número de serviços com dados pessoais inventariados/número de serviços com dados pessoais do órgão * 100

4. Índice de quantidade de controles de segurança e privacidade implementados para um determinado serviço:

Indicador	Descrição	Fórmula de Cálculo
Índice de quantidade de controles de segurança e privacidade implementados para os serviços	Acompanhar o processo de implementação de controles de segurança para os serviços. Medição: anual	Quantidade de controles de segurança e privacidade implementadas para um determinado serviço/quantidade total de controles de segurança e privacidade identificados para o serviço * 100.

3.3.2 GESTÃO DE INCIDENTES

Um incidente de segurança com dados pessoais é 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, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais.

Conforme estabelecido no inciso I, § 2º, do art. 50, da LGPD, será confeccionado um Plano de Resposta a Incidentes, de acordo com o modelo do ANEXO D, deste Programa, que será elaborado pelo Encarregado de dados do HFA.

Visando complementar o Plano de Resposta a Incidentes será confeccionado, também, o Plano de Comunicação, que será elaborado pelo Encarregado de dados do HFA. O Plano de Comunicação tem o objetivo de orientar a forma que os incidentes de segurança, que acarretem risco ou dano, sejam informados aos órgãos fiscalizatórios, aos titulares de dados e à imprensa.

3.3.3 ANÁLISE E REPORTE DE RESULTADOS

Buscando o reporte dos resultados obtidos e evolução das ações, bem como reforçar e fortalecer a cultura de privacidade dos dados. Todos os marcos realizados ou concluídos deste Programa serão publicados em Boletim Interno do HFA, e os resultados dos indicadores de performance serão monitorados e compilados no Plano Anual de Controle Interno (PACI) da Assessoria de Controle Interno do HFA.

Assim como, a divulgação na página da intranet do HFA de matéria sobre as medidas tomadas para implementação da segurança e privacidade de dados pessoais prevista neste Programa.

4 REVISÃO

Este programa deverá ser revisado a cada 2 (dois) anos ou sempre que determinado pelo Controlador e revisado pelo Comitê de Governança Digital, Privacidade e Segurança da Informação do HFA.

5 REFERÊNCIAS BIBLIOGRÁFICAS

- 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);
- Instrução Normativa Nº 1, de 27 de maio de 2020: Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal (GSI);
- Instrução Normativa SGD/ME Nº 117, de 19 de novembro de 2020, dispõe sobre Instrução normativa SGD/ME Nº 117, de 19 de novembro de 2020, dispõe sobre da administração pública federal direta, autárquica e fundacional;
- Orientação Normativa Nº 05/CMT LOG HFA, de 15 de agosto de 2019. Publicado no BI nº 160/HFA, de 20 AGO 19 que dispõe sobre a Política de Segurança da Informação e Comunicações do Hospital das Forças Armadas (POSIC/HFA);
- Portaria GM-MD Nº 5.814, de 29 de novembro de 2022. Dispõe sobre a Diretriz para a Proteção de Dados Pessoais no Ministério da Defesa;
- 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
- Cavoukian, Ann (2009). "Privacy by Design: Os 7 Princípios Fundamentais" (PDF). Escritório do Comissário de Informação e Privacidade de Ontário. Acesso em 7 de julho de 2023.

6 ANEXOS

Anexo A - Modelo de Mapeamento e inventário de dados pessoais.

Anexo B - Modelo de Relatório de impacto à proteção de dados pessoais.

Anexo C - Modelo do Termo de Uso e Aviso de Privacidade.

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

7 APROVAÇÃO

Brasília, DF, 5 de setembro de 2023.

Gen Div JORGE ROBERTO LOPES FOSSI
Comandante Logístico do Hospital das Forças Armadas

"HFA: Unindo Forças pela Saúde""

Histórico de Versões

VERSÃO	DATA	DESCRIÇÃO	AUTOR
1.0	31/08/2023	Primeira versão do Programa de Gestão em Privacidade	Equipe Técnica de Elaboração


HFA
HOSPITAL DAS FORÇAS ARMADAS
UNINDO FORÇAS PELA SAÚDE
www.gov.br/hfa
hfasaude
Assessoria de
Controle Interno (ACI)