



Fundação PATRIA
Fundação Parque de Alta Tecnologia
da Região de Iperó e Adjacências

Ministério da Ciência, Tecnologia e Inovações
Marinha do Brasil
Prefeitura Municipal de Iperó
CNPJ 71.558.068/0001-39
Inscrição Estadual 358.066.586.112

PORTARIA Nº 026/2025/PATRIA, NA DATA DE ASSINATURA.

Dispõe sobre a emissão de Normas Administrativas da Fundação PATRIA.

O DIRETOR-PRESIDENTE DA FUNDAÇÃO PARQUE DE ALTA TECNOLOGIA DA REGIÃO DE IPERÓ E ADJACÊNCIAS, no uso de suas atribuições legais constantes no Art. 30, Inciso VIII, Alínea f do Regimento Interno 8ª Revisão, resolve:

Art. 1º Colocar em vigor a Norma Administrativa DA – NA – 014 – 00 – Norma de Proteção de Dados Pessoais, anexa a esta Portaria, no âmbito da Fundação Parque de Alta Tecnologia da Região de Iperó e Adjacências (PATRIA).

Art. 2º Esta Portaria entra em vigor na presente data.

ANTONIO BERNARDO FERREIRA
Diretor-Presidente

Distribuição: Todos os elementos organizacionais da Fundação, Arquivo.



NORMA DE PROTEÇÃO DE DADOS PESSOAIS

CONTROLE DE MODIFICAÇÕES

Modificação	Data	Documento que modifica
00	28/07/2025	Portaria 026/2025
Itens modificados		
Emissão inicial		

Modificação	Data	Documento que modifica
Itens modificados		

SUMÁRIO**1 – PROPÓSITO****2 – APLICAÇÃO****3 – FUNDAMNETOS LEGAIS****4 – DEFINIÇÕES****5 – RESPONSABILIDADES****6 – DOS PRINCÍPIOS****7 – BASES LEGAIS PARA O TRATAMENTO DE DADOS PESSOAIS****8 – DOS DIREITOS DO TITULAR****9 – DO TRATAMENTO DOS DADOS****10 – ISENÇÃO DE RESPONSABILIDADE****11 – AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS****12 – ENCARREGADO DE TRATAMENTO DE DADOS PESSOAIS (CONTROLADOR)****13 – ENCARREGADO DA PROTEÇÃO DE DADOS****14 – COMITÊ DE PROTEÇÃO DE DADOS****15 – DISPOSIÇÕES GERAIS****16 – VIGÊNCIA****17 – DISTRIBUIÇÃO****ANEXOS****Anexo I - Termo de Consentimento Para Tratamento de Dados Pessoais****Anexo II – Modelo de Relatório de Impacto à Proteção de Dados Pessoais (RIPD)**

1 – PROPÓSITO

Definir os procedimentos, as atribuições e as responsabilidades para o tratamento dos dados pessoais realizados pela Fundação em conformidade com a Lei Geral de Proteção de Dados (LGPD).

2 – APLICAÇÃO

Esta Norma é aplicada aos envolvidos no tratamento dos dados pessoais, incluindo os Empregados da Fundação PATRIA, os funcionários e os empregados das entidades apoiadas e das empresas que por ventura venham a ser operadoras de dados desta Fundação.

3 – FUNDAMENTOS LEGAIS

São fundamentos legais a serem seguidos:

Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) - promulgada para proteger os direitos fundamentais de liberdade e privacidade e a livre formação da personalidade de cada indivíduo. Versa sobre o tratamento de dados pessoais, dispostos em meio físico e digital, feito por pessoa física ou jurídica de direito público ou privado;

Lei nº 9.307, de 23 de setembro de 1996, Lei da arbitragem; e

DA - NA - 011 - 00 - Norma de Segurança das Informações.

4 – DEFINIÇÕES

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;

Titular: pessoa física ou jurídica a quem se referem os dados pessoais que são objeto de tratamento;

Agentes de tratamento: o controlador e o operador;

Controlador: pessoa física ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais. No caso aqui, pessoa jurídica, o Diretor-Presidente responde pela Fundação como Controlador;

Operador: pessoa física ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do Controlador. No caso aqui, o escritório de contabilidade terceirizado;

Dado Pessoal: informação relacionada a pessoa física identificada ou identificável;

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, saúde ou vida sexual, genético ou biométrico, quando vinculado a uma pessoa física;

Relatório de Impacto à Proteção de Dados Pessoais (RIPD): deve ser elaborado preferencialmente antes do início do tratamento de dados pessoais, especialmente em projetos ou processos que possam gerar riscos às liberdades civis e direitos fundamentais dos indivíduos.

O RIPD é um documento estratégico que avalia e documenta os potenciais impactos das operações de tratamento de dados pessoais, auxiliando as organizações a identificar e mitigar riscos à privacidade.

Banco de Dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, com suporte eletrônico ou físico;

Eliminação: exclusão de um dado ou de um conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

Empregado: aquele que possui contrato de trabalho com a Fundação PATRIA;

Encarregado da Proteção de Dados (EPD): pessoa indicada pelo Controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD. No caso aqui, o EPD é o Gerente de Segurança Corporativa;

Transferência Internacional de Dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

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; e

Usuário: Empregado que está autorizado a obter acesso a informações, sistemas de computação ou redes de computadores da Fundação PATRIA.

5 – RESPONSABILIDADES

Controlador: Elaborar RIPDP; manter registro das operações de tratamento de dados pessoais; e orientar o operador quanto ao tratamento de dados segundo instruções internas, da legislação vigente e das regulamentações da ANPD.

Encarregado (DPO): Receber as reclamações e comunicações dos titulares, responder e adotar providências; receber as comunicações da ANPD e adotar as providências necessárias; orientar todos os empregados sobre as práticas a serem tomadas em relação à proteção de dados pessoais; e executar outras atribuições determinadas pelo Controlador ou estabelecidas em normas complementares estabelecidas pela ANPD.

6 – DOS PRINCÍPIOS

As atividades de tratamento de dados pessoais deverão ser regidas pelos seguintes princípios:

Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

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;

Não Discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

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;

Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

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;

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.;

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; e

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.

7 – BASES LEGAIS PARA O TRATAMENTO DE DADOS PESSOAIS

A LGPD prevê as hipóteses que autorizam o tratamento de dados, bem como estão estabelecidos os requisitos para a execução destes procedimentos, sendo chamadas de bases legais de tratamento de dados pessoais, quais sejam:

- Mediante o fornecimento de consentimento pelo titular (ver Anexo I);
- Para o cumprimento de obrigação legal ou regulatória pelo controlador;
- Pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres;
- Para a realização de estudos por órgão de pesquisa, garantida o anonimato, sempre que possível;
- Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
- Para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei de Arbitragem;
- Para a proteção da vida ou da incolumidade física do titular ou de terceiros;
- Para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
- Quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; e
- Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

8 – DOS DIREITOS DO TITULAR

A LGPD garante ao titular dos dados pessoais, junto ao controlador, a qualquer momento e mediante requisição, o direito:

- Confirmar a existência de tratamento;
- Acessar os dados;
- Corrigir de dados incompletos, inexatos ou desatualizados;
- Bloquear ou eliminar dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei;
- Exercer 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;
- Eliminar dados pessoais tratados com o consentimento do titular;
- Ser informado sobre entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
- Ser informado sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
- Revogar qualquer consentimento;
- Peticionar em relação aos seus dados contra o controlador perante a autoridade nacional;
- Opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto na Lei;
- 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 controlador deverá fornecer, sempre que solicitado, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.

Em caso de não oferecimento de informações baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

9 – DO TRATAMENTO DOS DADOS

É toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, compartilhamento, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

9.1 – No Armazenamento

9.1.1 – Digital

A Fundação possui proteção cibernética contra invasões por hackers, realizada através de Firewall e Sistema de Detecção de Intrusão (IDS – Intrusion Detection System) que

diuturnamente zelum pela segurança das informações digitais.

Cópias de segurança dos sistemas são realizadas, pela gerência de TIC, diariamente em Storage e armazenadas em local à parte do Data Center da Fundação.

Nas estações de trabalho, a guarda, armazenamento e a segurança, estão sob a responsabilidade do usuário da máquina conforme consta na Norma de Segurança da Informação Digital.

9.1.2 Físico

Documentos físicos deverão ser guardados em armários, arquivos, cofres ou qualquer outro suporte físico com fechamento por chave, a qual só terá acesso o pessoal do setor.

O setor deverá emitir Orientação Técnica correspondente, assinalando os procedimentos, responsabilidades, ações em caso de extravio e forma de garantir a integridade dos documentos armazenados.

9.2 Na Coleta

Os seguintes dados coletados dos empregados são utilizados para as finalidades a seguir:

Acesso à rede: nome, CPF, número de matrícula e endereço lógico do computador;

Administrativa: nome, endereço residencial, e-mail particular e número do WhatsApp;

Estatísticas: data de nascimento, idade, gênero e dependentes; e

Financeiras: nome, CPF e conta bancária.

9.3 No Compartilhamento

O compartilhamento de dados pessoais dos empregados com terceiros, na maioria dos casos, se deve ao cumprimento de obrigação legal ou regulatória, a saber:

- na inclusão de benefícios, com a finalidade de atender a acordos coletivos e/ou requisitos contratuais. O setor responsável (Seção de Recursos Humanos) deve emitir Orientação Técnica específica assinalando os procedimentos, responsabilidades e ações em caso de extravio, de forma a garantir a integridade dos dados compartilhados;

- na contratação de empresas ou nos convênios com parceiros, a Fundação PATRIA deve resguardar sua posição de controladora dos dados pessoais dos titulares envolvidos nos acordos e explicitar nos contratos/acordos cláusulas que evidenciem as responsabilidades da proteção e privacidade dos dados compartilhados;

9.4 Na Eliminação

Exceto nas situações previstas no artigo 16 da LGPD, a eliminação dos dados se dará quando:

- A ANPD determinar;
- Findar a finalidade para o qual o dado foi coletado;
- Findar temporalidade legal do dado armazenado; ou

- For solicitado pelo titular do dado.

10 – ISENÇÃO DE RESPONSABILIDADE

Apesar de adotar o que preconiza a LGPD e seguir os preceitos da Norma de Segurança da Informação Digital desta Fundação, a Fundação PATRIA não se responsabiliza por:

- Quaisquer consequências decorrentes da negligência, imprudência ou imperícia dos usuários em relação a seus dados individuais. Garantimos e nos responsabilizamos apenas pela segurança dos processos de tratamento de dados e do cumprimento das finalidades descritas no presente instrumento. Ressalta-se que a responsabilidade em relação à confidencialidade dos dados de acesso aos sistemas é do usuário;
- Ações maliciosas de terceiros, tais como: ataques de hackers, cópias não autorizadas e extravio de equipamentos;
- Inveracidade das informações inseridas pelo usuário nos bancos de dados da Fundação PATRIA. Quaisquer consequências decorrentes de informações falsas ou inseridas de má-fé são de inteira responsabilidade do usuário; e

Em caso de incidentes de segurança que possam gerar dano ao titular dos dados, esse incidente será comunicado aos envolvidos e à ANPD, de modo que sejam cumpridas as providências legais e necessárias.

11 – AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD)

As atividades que competem à referida Autoridade Nacional, estão descritas no Art. 55 da LGPD, sendo válido destacar as de maior relevância:

- Zelar pela proteção dos dados pessoais, nos termos da legislação;
- Elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade;
- Fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;
- Apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação;
- Promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança;
- Editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre o RIPDP para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na Lei; e
- Deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação da Lei, as suas competências e os casos omissos.

12 – ENCARREGADO DO TRATAMENTO DE DADOS PESSOAIS (CONTROLADOR)

A LGPD estabelece a obrigação do controlador em indicar um encarregado pelo tratamento de dados pessoais, cujas atividades são as seguintes:

- Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
- Receber comunicações da autoridade nacional e adotar providências;
- Comunicar à ANPD e ao titular a ocorrência de incidente de segurança que possa acarretar, risco ou dano relevantes aos titulares, conforme orientações adicionais da Autoridade.
- Orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;
- Indicar encarregado pelo tratamento de dados pessoais (DPO), que atuará como canal de comunicação entre o controlador, os titulares de dados e a ANPD;
- Implementar medidas de segurança técnicas e organizacionais adequadas a garantir segurança dos dados pessoais;
- Estar preparado para elaborar RIPDP conforme venha a ser determinado pela ANPD. Um modelo de RIPDP consta do Anexo II e inclui todas as instruções e referências necessárias à sua elaboração; e
- Manter registro do tratamento de dados das operações que realizar, especialmente quando baseado em legítimo interesse.

13 – ENCARREGADO DE PROTEÇÃO DE DADOS (EPD)

De modo que o titular do dado, conforme descrito no item 9 desta Norma, possa exercer seus direitos e para que todos os empregados sanem suas dúvidas sobre a LGPD, a Fundação disponibiliza o e-mail abaixo para contato com o EPD:

E-mail : lgpd@patria.org.br

A LGPD estabelece quatro funções para o EPD que são:

- Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
- Receber comunicações da autoridade nacional e adotar providências. O encarregado também será o mediador entre a empresa e o governo. Ele receberá os comunicados da ANPD e adotará as devidas providências;
- Orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
- Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

14 – COMITÊ DE PROTEÇÃO DE DADOS

De forma a possibilitar ações coordenadas e manter em vigor o que é estabelecido na LGPD, a

instituição de um Comitê de Proteção de Dados. O Comitê apoia o EPD no atendimento aos titulares de dados, nas demandas da ANPD e na adequação da Fundação à LGPD.

O Comitê de Proteção de Dados tem na sua composição: EPD, GIRCI, Encarregado da Seção de recursos Humanos, um representante da Assessoria Jurídica e um Gerente da Diretoria Técnica.

15 - DISPOSIÇÕES GERAIS

Inobstante ser a Fundação PATRIA entidade privada sem fins lucrativos, os conceitos e condutas listados nesta norma são recomendados e regulamentados de acordo com a Lei 13.709/2018 (LGPD).

16 – VIGÊNCIA

Esta Norma entra em vigor na presente data.

17 – DISTRIBUIÇÃO

Todos os elementos organizacionais da Fundação, sítio eletrônico da Fundação, Arquivo.

Anexo I

TERMO DE CONSENTIMENTO PARA TRATAMENTO DE DADOS PESSOAIS

Em conformidade com o previsto na Lei nº 13.709, de 2018, Lei Geral de Proteção de Dados Pessoais – LGPD, o (a) Empregado (a) Sr. (a) _____, portador da CTPS nº _____, Série _____, inscrito no CPF sob o nº _____, doravante denominado (a) **Titular**, registra sua manifestação livre e informada, concordando com o tratamento de seus dados pessoais, para a finalidade informada neste instrumento, pela Fundação PATRIA, doravante denominada **Controladora ou Empregadora**, para que esta, de acordo com a finalidade, tome as decisões em relação aos seus dados pessoais, envolvendo 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.

Cláusula Primeira – Dados Pessoais que serão tratados pela Controladora - Empregadora:

1.1. A Controladora fica autorizada a tomar decisões relativas ao tratamento dos seguintes dados pessoais do (a) Titular.

- Nome completo, inclusive o nome social;
- Data de Nascimento;
- Número e Imagem da Carteira de Identidade (RG);
- Número e imagem do Cadastro de Pessoas Físicas (CPF);
- Número e Imagem da Carteira Nacional de Habilitação (CNH);
- Fotografia 3x4;
- Estado Civil;
- Tipo Sanguíneo e fator RH;
- Nível de instrução ou Escolaridade;
- Endereço Completo;
- Número de Telefone, WhatsApp e endereço de correio eletrônico (e-mail);
- Nome dos filhos, inclusive as datas de nascimento e informações dos atestados de vacinação;
- Filiação;
- Dados bancários;
- Atestados Médicos;
- Situações conjugais que possam ter reflexos nas relações de trabalho, como pagamento de pensão alimentícia e inclusão de dependente em plano de saúde;

Cláusula Segunda – Finalidades específicas do tratamento dos dados pessoais do (a) Titular:

2.1. O tratamento dos dados pessoais listados no presente termo tem as seguintes finalidades específicas:

- a) Possibilitar que a Empregadora faça a formalização do contrato de trabalho, com base na Consolidação das Leis do Trabalho – CLT;
- b) Possibilitar que a Empregadora cumpra com as exigências legais de registros obrigatórios na CTPS física ou digital, bem como no eSocial;
- c) Possibilitar que a Empregadora faça os registros relativos à manutenção do vínculo de emprego e execução do contrato de trabalho em livros, fichas ou arquivos eletrônicos;
- d) Possibilitar que a Empregadora realize o pagamento do salário-família, quando cabível para a função;
- e) Possibilitar que a Empregadora realize a aquisição do vale-transporte;
- f) Possibilitar que a Empregadora realize a emissão de recibos de pagamento de salário, férias, décimo-terceiro e demais benefícios previstos no Acordo Coletivo de Trabalho – ACT;
- g) Possibilitar que a Empregadora cumpra exigências legais relativas à saúde do trabalhador, com vistas à realização de exames médicos, admissional, periódico e demissional;
- h) Possibilitar que a Empregadora possa utilizar os dados para encaminhar correspondências e mensagens por meios físicos e digitais, abrangendo correio eletrônico (e-mail) e WhatsApp, inclusive para fazer a inclusão em grupos de WhatsApp da empresa;

Cláusula Terceira – Período do Tratamento dos Dados Pessoais

3.1. Os dados pessoais coletados serão tratados e armazenados pela Controladora nas seguintes hipóteses:

- Enquanto perdurar a relação de emprego;
- Até a revogação pelo (a) Titular;
- Enquanto necessário para atender prazos legais e regulatórios.

3.2. A Controladora poderá manter e tratar os dados pessoais do (a) Titular durante todo o período em que os mesmos forem pertinentes ao alcance das finalidades listadas neste instrumento, sendo que os dados pessoais anonimizados, sem possibilidade de associação ao (à) Titular, poderão ser mantidos por período indeterminado.

3.3. O (A) Titular poderá solicitar a Controladora, a qualquer tempo, por meio de correio eletrônico (e-mail) ou correspondência, que sejam eliminados seus dados pessoais não anonimizados.

3.4. A partir da eliminação dos dados pessoais, o (a) Titular se declara ciente de que poderá restar inviabilizado o contato e o encaminhamento de mensagens e correspondências da Controladora para o (a) Titular.

3.5. A partir da eliminação dos dados pessoais, o (a) Titular se declara ciente de que poderá restar inviabilizado o cumprimento das finalidades descritas na cláusula segunda, item 2.1 deste Termo, sob conta e risco do (a) Titular.

Cláusula Quarta – Compartilhamento de dados

4.1. A Controladora fica autorizada a compartilhar os dados pessoais do (a) Titular com outros agentes de tratamento de dados, inclusive órgãos públicos, em caso de necessidade e para as finalidades listadas na cláusula segunda, item 2.1, observados os princípios e as garantias estabelecidas na Lei nº 13.709, de 2018.

4.2. A Controladora fica autorizada a compartilhar os dados pessoais do (a) Titular nas situações que

envolverem convênios médicos, planos de saúde, vale-refeição, vale-alimentação, consultorias contratadas, SESMT e informações alusivas às obrigações fiscais, previdenciárias e trabalhistas.

Cláusula Quinta – Segurança dos dados

5.1. Em conformidade com o artigo 48 da Lei nº 13.709, de 2018, a Controladora comunicará ao (à) Titular e à Autoridade Nacional de Proteção de Dados (ANPD) a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante ao (à) Titular.

Cláusula Sexta – Direitos do (a) Titular:

6.1. O (A) Titular tem direito de obter do Controlador, em relação aos dados pessoais por ela tratados, a qualquer tempo, e mediante requisição expressa:

- a) Confirmação da existência do tratamento;
- b) Acesso aos dados pessoais;
- c) Correção de dados incompletos, inexatos ou desatualizados;
- d) Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei Geral de Proteção de Dados Pessoais;
- e) Portabilidade dos dados a outro fornecedor de produto ou serviço, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
- f) Eliminação dos dados pessoais tratados com o consentimento do (a) Titular, exceto nas hipóteses previstas no art. 16 da Lei nº 13.709, de 2018;
- g) Informação das entidades públicas e privadas com as quais o Controladora realizou o uso compartilhado dos dados;
- h) Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
- i) Revogação do Consentimento, nos termos do § 5º do art. 8º da Lei nº 13.709, 2018;

Iperó, ____ de _____ de _____.

Assinatura do Empregado

Anexo II**MODELO DE RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS****Histórico de Revisões**

Data	Versão	Descrição	Autor
XX/XX/20X X	1.0	Conclusão da primeira versão do relatório	XXXXXXXXXX XX
XX/XX/20X X	2.0	Revisão do relatório após análise do controlador, operador e encarregado.	XXXXXXXXXX XX

ATENÇÃO!

<Os trechos marcados em azul neste template são editáveis, notas explicativas ou exemplos, devendo ser substituídos ou excluídos, conforme necessário>.

OBJETIVO

O Relatório de Impacto à Proteção de Dados Pessoais 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.

Referência: Art. 5º, XVII da Lei 13.709/2018 (LGPD).

1 – IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO**Controlador**

<Nome da pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (LGPD, art. 5º, VI)>.

Operador

<Nome da pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (LGPD, art. 5º, VII)>.

Encarregado

<Nome da 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 (LGPD, art. 5º, VIII).>

E-mail Encarregado	Telefone Encarregado
<xxxx.xxxx.gov.br>	<(99)9999-9999>

2 – NECESSIDADE DE ELABORAR O RELATÓRIO

<Os casos específicos previstos pela LGPD em que o 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 LGPD em decorrência do tratamento de dados pessoais por órgãos públicos (arts. 31 e 32 combinados); e
- a qualquer momento sob determinação da ANPD (art. 38).>

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

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

<Além dos casos específicos previstos pela LGPD no início desta seção 2 relativas à elaboração do RIPD, é indicada a elaboração ou atualização do Relatório de Impacto sempre que existir a possibilidade de ocorrer impacto na privacidade dos dados pessoais, resultante de:

- uma tecnologia, serviço ou outra nova iniciativa em que dados pessoais e dados pessoais sensíveis sejam ou devam ser tratados;
- rastreamento da localização dos indivíduos ou qualquer outra ação de tratamento que vise a formação de perfil comportamental de pessoa natural, se identificada (LGPD, art. 12 § 2º);
- tratamento de dado pessoal sobre “origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural” (LGPD, art. 5º, II);
- processamento de dados pessoais usado para tomar decisões automatizadas que possam ter efeitos legais, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade (LGPD, art. 20);
- tratamento de dados pessoais de crianças e adolescentes (LGPD, art. 14);
- tratamento de dados que possa resultar em algum tipo de dano patrimonial, moral, individual ou coletivo aos titulares de dados, se houver vazamento (LGPD, art. 42);
- tratamento de dados pessoais realizados para fins exclusivos de segurança pública, defesa nacional, segurança do Estado, ou atividades de investigação e repressão de infrações penais (LGPD, art. 4º, § 3º);
- tratamento no interesse legítimo do controlador (LGPD, art. 10, § 3º);
- alterações nas leis e regulamentos aplicáveis à privacidade, política e normas internas, operação do sistema de informações, propósitos e meios para tratar dados, fluxos de dados

novos ou alterados, etc.; e

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

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

3 – 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 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.>

3.1 – NATUREZA DO TRATAMENTO

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

<Importante descrever, por exemplo:

- como os dados pessoais são coletados, retidos/armazenados, tratados, usados e eliminados;
- fonte de dados (ex: titular de dados, planilha eletrônica, arquivo xml, formulário em papel, etc.) utilizada para coleta dos dados pessoais;
- com quais órgãos, entidades ou empresas os dados pessoais 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 da instituição.>

3.2 – 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.>

3.3 – 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 da organização com os indivíduos;
- nível ou método de controle que os indivíduos exercem sobre os dados pessoais;
- destacar se o tratamento envolve crianças, adolescentes ou outro grupo vulnerável;
- destacar se o tipo de tratamento realizado sobre os dados é condizente com a expectativa dos titulares dos dados pessoais. Ou seja, o dado pessoal não é tratado de maneira diversa do que é determinado em leis e regulamentos, e comunicado pela instituição ao titular de dados;
- destaque de qualquer experiência anterior com esse tipo de tratamento de dados;
- destaque de avanços relevantes da instituição em tecnologia ou segurança que contribuem para a proteção dos dados pessoais.>

3.4 – 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. 7º e 11 da LGPD), no que for aplicável:

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

<Cumpra-se destacar que os exemplos de finalidades apresentados neste documento não são exaustivos. Desse modo, deve-se informar e detalhar qualquer outra finalidade específica do controlador para tratamento dos dados pessoais, mesmo que tal finalidade não conste dos citados exemplos.

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

Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:

I - apoio e promoção de atividades do controlador; e

II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.

§ 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.

§ 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.

§ 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

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

4 – 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.>

5 – NECESSIDADE E PROPORCIONALIDADE

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

< Nesse sentido, destacar:

- A fundamentação legal para o tratamento dos dados pessoais.
 - Caso o fundamento legal seja embasado no legítimo interesse do controlador (LGPD, art. 10), demonstrar que:
 - esse tratamento de dados pessoais é indispensável;
 - não há outra base legal possível de se utilizar para alcançar o mesmo propósito; e
 - esse processamento de fato auxilia no propósito almejado.
 - Como será garantida a qualidade [exatidão, clareza, relevância e atualização dos dados] e minimização dos dados.
 - Quais medidas são adotadas a fim de assegurar que o operador (LGPD, art. 5º, VII) realize o tratamento de dados pessoais conforme a LGPD e respeite os critérios estabelecidos pela instituição que exerce o papel de controlador (LGPD, art. 5º, VI).
 - Como estão implementadas as medidas que asseguram o direito do titular dos dados pessoais obter do controlador o previsto pelo art. 18 da LGPD.
 - Como a instituição pretende fornecer informações de privacidade para os titulares dos dados pessoais.
 - Quais são as salvaguardas para as transferências internacionais de dados.>
- < O artigo 18 da LGPD é bem extenso e trata do direito que o titular tem de requisitar do controlador ações e informações específicas em relação ao tratamento realizado sobre os dados pessoais.>

6 – IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

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

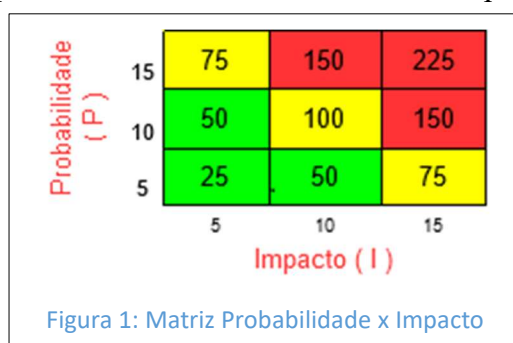
<Antes de definir tais medidas, salvaguardas e mecanismos, é necessário identificar os riscos que geram impacto potencial sobre o titular dos dados pessoais.>

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

<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.>

<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:

- verde, é entendido como baixo;
- amarelo, representa risco moderado; e
- 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 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 órgão preconizada pela **Instrução Normativa Conjunta MP/CGU nº 1, de 10 de maio de 2016**>.

Id	Risco referente ao tratamento de dados pessoais	P ¹	I ²	Nível de Risco (P x I) ³
R01	<Risco 1>			
R02	<Risco 2>			
R03	<Risco N>			

Legenda: P – Probabilidade; I – Impacto.

¹ 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).

² Impacto: resultado de um evento que afeta os objetivos (ISO/IEC 31000:2009, item 2.18).

³ 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).

<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 de cada instituição.** 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	10	15	150

	pessoais (Caso o tratamento não esteja previsto em legislação ou regulação pertinente).			
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
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

7 – 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 6 deste Relatório.>

<A instituição nem sempre precisa eliminar todos os riscos. Nesse sentido, pode-se decidir que alguns riscos são aceitáveis - até um risco de nível alto-, devidos 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 ANPD antes de prosseguir com as operações de tratamento dos dados pessoais.**>

Risco	Medida(s)	Efeito sobre o Risco ¹	Risco Residual ²			Medida(s) ³ Aprobada(s)
			P	I	Nível (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. Aplicam-se as mesmas definições de Probabilidade e Impacto da seção 6.

¹ 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.

² Risco residual é o risco que ainda permanece mesmo após a aplicação de medidas para tratar o risco.

³ Medida aprovada pelo controlador dos dados pessoais. Preencher a coluna com: Sim ou Não. <A seguir são apresentados exemplos de medidas para tratar os riscos a fim de demonstrar o preenchimento da tabela apresentada na página anterior>.

Risco	Medida(s)	Efeito sobre o Risco	Risco Residual			Medida(s) Aprovada(s)
			P	I	Nível (P x I)	
R01 Acesso não autorizado.	1. CONTROLE DE ACESSO LÓGICO	Reduzir	5	10	50	Sim
	2. DESENVOLVIMENTO SEGURO					
	3. SEGURANÇA EM REDES					
R04 Roubo.	1. CONTROLE DE ACESSO LÓGICO	Reduzir	5	5	25	Sim
	2. CONTROLES CRIPTOGRÁFICOS					
	3. PROTEÇÃO FÍSICA E DO AMBIENTE					
R06 Coleção excessiva.	1. Limitação da coleta.	Reduzir	5	10	50	Sim

8 – APROVAÇÃO

<Esta seção **visa formalizar a aprovação do RIPD** por meio da obtenção das assinaturas do Responsável pela elaboração do RIPD, pelo encarregado e pelas autoridades que representam o controlador e operador. O responsável pela elaboração do Relatório pode ser o próprio encarregado ou qualquer outra pessoa designada pelo controlador com conhecimento necessário para realizar tal tarefa>.

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

Detalhes sobre a necessidade de revisão do RIPD podem ser observados no **item 2.5.2.9 do Guia de Boas Práticas LGDP, disponível em:** <https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-lgpd.pdf> (link não funciona)

RESPONSÁVEL PELA ELABORAÇÃO DO RELATÓRIO DE IMPACTO	ENCARREGADO
<p>_____</p> <p><Nome do responsável></p> <p><Local>, <dia> de <mês> de <ano></p>	<p>_____</p> <p><Nome do encarregado></p> <p><Local>, <dia> de <mês> de <ano></p>

AUTORIDADE REPRESENTANTE DO CONTROLADOR	AUTORIDADE REPRESENTANTE DO OPERADOR
<hr/> <p><Nome do representante> <Local>, <dia> de <mês> de <ano></p>	<hr/> <p><Nome do representante> <Local>, <dia> de <mês> de <ano></p>

Relatório de Impacto à Proteção de Dados Pessoais (RIPD)

https://www.gov.br/guias/guia_template_ripd (link não funciona)