UNIRIO
UNIVERSIDADE FEDERAL DO ESTADO DO RIO DE JANEIRO

Guia de Boas Práticas da LGPD na UNIRIO

2024
Versão 01

FICHA TÉCNICA

Equipe Técnica de Elaboração

Isabela Costa da Silva (Diretora do Arquivo Central/ Encarregada pelo tratamento de dados pessoais da UNIRIO, Portaria GR nº 801, de 06/10/2023),
Fabiana da Costa Ferraz Patueli Lima,
Paulina Aparecida Marques Vieira Albuquerque.

Revisão técnica do CP-DADOS

Bruno Carvalho Da Silva,
Graziella Cataldo Batista Felix,
Heloisa Carneiro De Campos Moreira Amaral,
Jacqueline Dias da Silva,
Mariana Buarque Araujo,
Patrícia Machado Goulart França,
Sidney Cunha de Lucena,
Simone Borges Paiva Okuzono,
Vinícius José Serva Pereira.

Controle de versões

1ª versão em Junho de 2024.

U58 Universidade Federal do Estado do Rio de Janeiro.
Guia de boas práticas da LGPD na UNIRIO / Universidade Federal do Estado do Rio de Janeiro ; [Equipe técnica de elaboração: Isabela Costa da Silva, Fabiana da Costa Ferraz Patueli Lima, Paulina Aparecida Marques Vieira Albuquerque]. – Rio de Janeiro : UNIRIO, 2024.
1 E-book (25 p.)

1. Brasil. [Lei geral de proteção de dados pessoais (2018)].
2. Proteção de dados - Guias. 3. Direito à privacidade.
I. Universidade Federal do Estado do Rio de Janeiro. II. Silva, Isabela Costa da. III. Lima, Fabiana da Costa Ferraz Patueli.
IV. Albuquerque, Paulina Aparecida Marques Vieira. V. Título.

CDD – 342.810858

SUMÁRIO

1. APRESENTAÇÃO

Com a promulgação da Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709, de 14 de agosto de 2018, e sua atualização pela Lei nº 13.853, de 8 de julho de 2019, e a Emenda Constitucional nº 115, de 10 de fevereiro de 2022, que inclui a proteção de dados pessoais entre os direitos e garantias fundamentais, torna-se essencial assegurar que os procedimentos da Universidade Federal do Estado do Rio de Janeiro (UNIRIO) estejam em consonância com as disposições normativas legais quanto ao tratamento de Dados Pessoais.

A Universidade, enquanto Fundação ligada ao Ministério da Educação (MEC), do Poder Executivo Federal, é responsável pelo tratamento de dados pessoais de discentes, de sua força de trabalho, dos participantes diretos e indiretos dos projetos de ensino, de pesquisa, de inovação, de extensão e de cultura. Com isso, não podemos esquecer que a LGPD, bem como os seus entendimentos, visam garantir, ao titular ou à titular, segurança no tratamento de seus dados, e, à Universidade, o fluxo de informações necessárias à formação, ao desenvolvimento, à interação social e cultural de toda comunidade universitária.

O grande volume de dados pessoais e de dados pessoais sensíveis a serem administrados pela Universidade são uma das principais motivações para o presente instrumento, tornando-se necessárias orientações gerais que possam fundamentar boas práticas quanto ao tratamento de tais dados em seu âmbito, assim como o compromisso institucional quanto à sua proteção.

Por isso, o presente instrumento foi elaborado tendo como base: a LGPD (2018); o *Guia de Boas Práticas para Implementação na Administração Pública Federal*, do Comitê Central de Governança de Dados do Governo Federal (2020); o *Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado*, da Autoridade Nacional de Proteção de Dados (ANPD, 2022); o *Relatório do GT sobre a LGPD* da UNIRIO (2022); a Cartilha sobre a LGPD na UNIRIO (2023); e o *Guia Orientativo Tratamento de dados pessoais para fins acadêmicos e para a realização de estudos e pesquisas* (ANPD, 2023).

2. OBJETIVOS

O ***Guia de boas práticas da LGPD na UNIRIO*** têm como objetivos orientar a comunidade acerca dos aspectos gerais da aplicação da LGPD no âmbito da Universidade, esclarecer os papéis dos atores no âmbito da legislação e da UNIRIO, bem como sugerir as principais estratégias para o tratamento de dados pessoais no contexto da Universidade, visando a segurança dos seus dados e transparência dos procedimentos administrativos.

3. DEFINIÇÕES DE DADOS, INFORMAÇÕES E DOCUMENTOS

A LGPD considera **dados pessoais** as informações que possam identificar uma pessoa natural de forma direta ou indireta, conforme artigo 5º, inciso I, da LGPD. Assim, são exemplos de dados pessoais: **nome, sobrenome, data de nascimento, CPF, número de identificação civil ou militar, número da CNH, número da carteira de trabalho, número do passaporte, número do título de eleitor.**

Contudo, entende-se que na identificação de agentes públicos, bem como de sua competência, no exercício de suas atividades, alguns dados são publicizáveis, seja para validação do ato administrativo ou da instituição de fé pública, tais como: nome completo, matrícula, cargo ou função, assinatura.

Os **dados pessoais sensíveis** são definidos pela LGPD, quando vinculados a uma pessoa natural, como dados pessoais 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, conforme artigo 5º, inciso II, da LGPD.

Assim, entende-se como **informação** o elemento referencial, noção ou ideia contidos num documento. E **banco de dados** como sendo o conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico, de acordo com o artigo 5º, inciso IV, da LGPD, que por sua vez é ele mesmo um documento.

Na Universidade, os serviços e as atividades são manifestados por meio da produção de **documentos,** que podem ser de várias espécies e tipos, independente do seu formato (analógico ou digital), tais como: Acordo/Termo de Cooperação, Ata, Cerimonial, Declaração, Despacho, Edital, Estatuto, Instrução Normativa, Ofício - Comunicação Interna, Ofício - Comunicação Externa, Portaria, Portaria com Atos de Pessoal, Regimento, Regulamento, Resolução, ou Resolução *ad referendum*, conforme o *Manual de Atos Oficiais da UNIRIO* e o *Manual da Presidência da República*. Diante do exposto, considera-se informação aquilo que se depreende da leitura dos documentos, que podem conter dados que identifiquem direta ou indiretamente uma pessoa natural, tratados no interesse da Administração Pública para efetivação de suas atividades.

Além disso, há os dossiês e processos administrativos, que são tipologias documentais que se constituem por conjunto de documentos relacionados entre si por assunto e por conjunto de documentos oficialmente reunidos no decurso de uma ação administrativa, respectivamente.

Assim, na Universidade, tais espécies e tipologias documentais podem conter dados pessoais e dados pessoais sensíveis que precisam ser tratados em razão de finalidade inerentes às atividades e aos serviços públicos que a instituição oferece. Contudo, a divulgação de tais informações deve respeitar o direito do titular ou da titular de dados pessoais e sempre que possível se utilizar de meios técnicos razoáveis de anonimização, tarjamento ou restrição de acesso aos dados pessoais.

4. ATRIBUIÇÃO DE PAPÉIS E RESPONSABILIDADES

É importante salientar que a LGPD precipuamente define os papéis dos beneficiários e dos demais agentes em seu próprio texto, entre os quais temos os indivíduos, os agentes de tratamento (controlador e operador)[1], o encarregado e a integração com as demais organizações, sejam públicas ou privadas. Diante desse escopo, é importante a descrição dos papéis mencionados, conforme os dispositivos que serviram de base para o presente Guia.

Entendendo que **o titular ou a titular** de dados é pessoa natural a quem se referem os **dados pessoais** que são objeto de tratamento, a UNIRIO trata dados pessoais dos seguintes usuários:

- Discentes;
- Servidores;
- Terceirizados;
- Pacientes;
- Parceiros;
- Integrantes da comunidade.

Aos titulares de dados pessoais cabe a cessão de consentimento por escrito quando lhes forem solicitados, excetuando à Administração Pública, desde que seja necessário para a prestação do serviço ou realização da atividade com finalidade certa e determinada.

Neste escopo, considera-se **controlador** de dados pessoais a pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais e sua finalidade. Assim, tem-se como controlador a própria UNIRIO, por considerar que realiza funções típicas do controlador, tendo em vista a desconcentração administrativa da estrutura da União.

Ao Controlador cabe:

- a elaboração de relatório de impacto à proteção de dados pessoais (artigo 38, da LGPD), quando solicitado pela Autoridade Nacional de Proteção de Dados (ANPD);
- a comprovação de consentimento obtido de titulares no atendimento de exigências legais (artigo 8, § 2º, da LGPD), quando houver exigência para tal;
- a comunicação à ANPD de ocorrência de incidentes de segurança (artigo 48, da LGPD);
- o fornecimento de informações a titulares de dados pessoais sobre o tratamento, quando requerido pelo mesmo;

[1] Observa-se que [início de citação] "Não são considerados controladores (autônomos ou conjuntos) ou operadores os indivíduos subordinados, tais como os funcionários, os servidores públicos ou as equipes de trabalho de uma organização, já que atuam sob o poder diretivo do agente de tratamento" [fim de citação] (GUIA ORIENTATIVO PARA DEFINIÇÕES DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS E DO ENCARREGADO, 2022, p. 7).

- a seguridade de correção de dados pessoais, quando lhe for requerido pelo titular ou pela titular de dados pessoais.

Operadores são considerados pessoas naturais ou jurídicas, de direito público ou privado, que realizam o tratamento de dados pessoais em nome do Controlador, que deverá verificar a observância das próprias instruções e das normas sobre a matéria (artigo 39, da LGPD). Na UNIRIO, por exemplo, os operadores são aqueles que, por motivos distintos, possuem acesso aos dados dos usuários, tais como fornecedores de bens e serviços, organização e instituições parceiras.

Assim, cabe aos operadores de dados pessoais:

- seguir as instruções do controlador;
- firmar contratos que estabeleçam, dentre outros assuntos, o regime de atividades e responsabilidades com o controlador;
- dar ciência ao controlador em caso de contrato com sub-operador.

Observa-se que os funcionários da UNIRIO apenas integram a força de trabalho das unidades organizacionais do ente controlador de dados, razão pela qual não se caracterizam como agentes de tratamento.

Encarregado ou Encarregada é a pessoa (física ou jurídica) indicada por um controlador, que atua como canal de comunicação entre este, os titulares e a ANPD, com as seguintes atribuições, conforme o artigo 41 da LGPD:

- aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
- receber comunicações da Autoridade Nacional e adotar providências;
- orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;
- executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Por ser a ponte entre as principais partes interessadas no tratamento de dados pessoais, os dados do encarregado, bem como os seus canais de comunicação, devem estar divulgados no sítio eletrônico da instituição. Na UNIRIO, o encarregado ou a encarregada é um servidor estável indicado pelo Gabinete da Reitoria e os seus dados estão disponíveis em: https://www.unirio.br/acessoinformacao/protecao-de-dados-pessoais.

Por fim, a **Autoridade Nacional de Proteção de Dados (ANPD)**, é autarquia especial[2] responsável por zelar, implementar e fiscalizar o cumprimento da LGPD, a quem o controlador deverá prestar informações direta ou por intermédio do encarregado, além de possibilitar mais um canal de comunicação com o cidadão.

[2] Transformou-se em autarquia especial com a promulgação da Lei nº 14.460, de 25 de outubro de 2022.

5. TRATAMENTO DE DADOS PESSOAIS

O tratamento de dados pessoais se trata de 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**, de acordo com o artigo 5, X, da LGPD. E as hipóteses legais que tornam possível o seu tratamento estão descritas no artigo 7 e 11 da LGPD.

Na Universidade, essas operações têm por finalidade uma atividade ou um serviço de interesse público, o que deverá estar explicitado. A conservação e a tramitação de dados pessoais contidos em documentos institucionais, bem como sua transferência para arquivo intermediário e a destinação final, quer seja o recolhimento para guarda permanente ou sua eliminação, são definidos por instrumentos de gestão de documentos - Plano de Classificação de Documentos de Arquivo (PCD) e os respectivos Códigos de Classificação de Documentos e Tabelas de Temporalidade e Destinação de Documentos (TTDD), relativos às Atividade-Meio e Atividade-Fim, do Conselho Nacional de Arquivos (Conarq).

De todo modo, devem ser garantidos a titulares de dados pessoais a observância da boa fé e os seguintes princípios do artigo 6 da LGPD, no tratamento de seus dados pessoais:

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.

O **tratamento de dados pessoais sensíveis** deverá ocorrer em conformidade com o artigo 11, da LGPD, e para tal sugere-se que a coleta deste tipo de dado, sempre que

possível, seja realizada em separado, tramitado e conservado com cautela, com a garantia, sempre que possível, de anonimização e pseudonimização no seu compartilhamento.

Observa-se que o acesso aos dados pessoais contidos nos documentos institucionais poderá ser realizado pelos próprios titulares ou por seus representantes legais. Já o acesso aos documentos institucionais, este poderá ser realizado pelas unidades da instituição para execução de sua finalidade e/ou atividade, ou por entidades de fiscalização e por cidadãos, no que tange à Lei nº 12.527/2011, Lei de Acesso à Informação (LAI). Para o acesso deste último, sugere-se o tarjamento de dados pessoais pelo prazo máximo de 100 anos, como forma de restrição, ou anonimização, ou pseudonimização, dos dados de pessoas naturais disponibilizados. Mas, observa-se que o tarjamento deverá ser utilizado somente sob a cópia de acesso aos documentos, preservando o original com todas as suas características e informações durante o seu respectivo prazo prescricional, conforme a temporalidade e destinação das Tabelas de Temporalidade e Destinação de Documentos do CONARQ.

Neste escopo, também é assegurado o papel dos acervos institucionais como [início de citação] “fontes de pesquisa científica, estatística, genealógica, histórica ou de evidente interesse público, assegurando-se a privacidade na divulgação dos resultados” [fim de citação], conforme artigo 4, VI, da Resolução Conarq nº 54, de 8 de dezembro de 2023. Por isso, na Universidade, a pesquisa externa aos acervos institucionais é viabilizada por meio de termo de responsabilidade.

Observa-se que o tratamento de dados pessoais de **crianças e adolescentes** deverá ser realizado, impreterivelmente, tendo em vista as hipóteses legais previstas, conforme está indicado no artigo 14 da LGPD:

> Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.
>
> § 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.
>
> § 2º No tratamento de dados de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o artigo 18 desta Lei.
>
> § 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo.
>
> § 4º Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras atividades, ao fornecimento de informações pessoais além das estritamente necessárias à atividade.
>
> § 5º O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis.
>
> § 6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível,

> consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

5.1. CONTROLE SOBRE OS AMBIENTES DE TRATAMENTO DE DADOS PESSOAIS

Os ambientes de tratamento de dados pessoais ou de dados pessoais sensíveis são os locais em que os dados são registrados e depositados, ou seja, em que se realiza o tratamento dos respectivos dados. Isso quer dizer que a instituição deve ter o controle sobre onde os dados estão depositados para adotar medidas de segurança para cada local de armazenamento e/ou processamento.

Observa-se que um documento de papel depositado em um arquivo corrente, tal como um sistema ou planilha eletrônica, pode ser um destes ambientes. Logo, é imprescindível que tanto as subunidades quanto a Universidade como um todo tenham tais ambientes rastreados.

Tendo-se em mente que o local de armazenamento, processamento e arquivamento de dados pessoais são estrategicamente importantes, pode-se aventar os riscos e as medidas de segurança que melhor se aplicam para cada situação.

Nesse escopo, são locais comuns de registro, trânsito de informações e, com isso, de dados pessoais, os seguintes exemplos: correio eletrônico/e-mail institucional e não institucional; portais da instituição; formulário/requerimentos em papel; formulário próprio digital com armazenamento em drive/nuvem; outros documentos em papel na Unidade; Sistema de Informação para o Ensino (SIE); Sistema Eletrônico de Informações (SEI); drive/nuvem institucional e não institucionais.

Observa-se que os **requisitos mínimos de *login* e perfis** para cada unidade e seus respectivos usuários já é um requisito mínimo de segurança seguido atualmente pela Universidade, que necessita de revisão a cada desligamento e/ou movimentação funcional a pedido dos responsáveis pelas unidades acadêmicas e administrativas. A cibersegurança dos sistemas, endereço eletrônico e *backups* de toda a UNIRIO são de responsabilidade da Diretoria de Tecnologia da Informação e Comunicação (DTIC/Proplan).

Já o acesso aos documentos analógicos (ex.: em papel) em cada arquivo, corrente, intermediário e permanente, é de responsabilidade dos respectivos funcionários das unidades, bem como quanto à sua disponibilização em qualquer meio. Por isso, o acesso deve ser avaliado caso a caso, tendo em vista a manutenção da privacidade e a Lei de Acesso à Informação (LAI, Lei n° 12.527, de 18 de novembro de 2011).

A responsabilidade de cada funcionário para segurança e manutenção da privacidade de dados pessoais e de pessoais sensíveis é um dever de todos e, muitas das vezes, poderá ter seus riscos minimizados com coletas de dados mais restritas à necessidade do serviço e à sua finalidade específica, calcada na hipótese legal da LGPD.

5.2. DIVULGAÇÃO DE DADOS PESSOAIS

A LGPD não suplanta as fiscalizações internas e externas junto à Instituição em suas respectivas atividades regulatórias, bem como o acesso da sociedade civil às informações necessárias para averiguação dos atos administrativos relacionado à Lei de Acesso à Informação, Lei n° 12.527, de 18 de novembro de 2011. Desta forma, faz-se necessário contrabalancear o respeito à privacidade e a transparência pública nos seguintes atos administrativos:

a) Lista de candidaturas para processos de seleção

Para a divulgação de listas de candidaturas à processos de seleção na Universidade, tanto para aprovados quanto reprovados/desistentes/faltosos, indica-se que:

- sejam utilizados o nome completo do candidato e o número de inscrição fornecido na candidatura;
- sejam utilizados o nome completo do candidato e o número de CPF, que deverá ser descaracterizado com asteriscos nos 3 primeiros e 3 últimos números (ex.: ***.XXX.XX*-**).

A padronização garantirá a publicização dos atos administrativos referentes ao concurso público, fornecendo informações mínimas para averiguação da sociedade sobre a matéria, sem com isso ser capaz de identificar uma pessoa natural, haja vista que, o nome completo por si só não identifica uma pessoa natural devido a possibilidade de homonímia., . E, por razoabilidade, este dado sozinho não seria capaz de legitimar o rito perante a órgãos de fiscalização e ao controle social da Administração Pública. Por isso, depreende-se que há a necessidade de combinação com dados secundários, tais como número de inscrição ou CPF pseudonimizado. Observa-se que o número de inscrição, também sem a combinação de outros documentos, não é capaz de identificar ou provocar danos à privacidade do titular de dados pessoais, bem como o número do CPF pseudonimizado.

b) Matrícula SIAPE do servidor

Atualmente, há o entendimento de que a matrícula, junto ao nome completo do agente público, pode ser divulgada, pois, dentre os dados solicitados para o mesmo no desempenho de suas funções, seria o menos invasivo, incapaz de provocar prejuízos em face do controle social possível à Administração Pública, especialmente em situações em que possa haver conflitos de interesse, conforme os entendimentos depreendidos do PARECER n. 00002/2023/CNMLC/CGU/AGU, Nota Técnica n. 85/2023/CGN/ANPD e PARECER n. 00001/2024/CNCIC/CGU/AGU.

c) Listagens de nomes de titulares de dados pessoais

Por se entender que se faz necessário vigorar a transparência de atos administrativos advindos das atividades regulatórias da Universidade são passíveis de divulgação o quantitativo, bem como listagens de nomes de servidores, discentes, colaboradores eventuais, terceirizados e assistidos, associados ou não aos seguintes dados: matrículas; área de ensino/aprendizagem; nomes de projetos de extensão,

cultura, pesquisa, inovação; título de tipologias e assuntos de processos administrativos e acadêmicos em que é parte relacionada (excetuando: assuntos de natureza pessoal sensível (Art. 5, II da LGPD), a processos de denúncia, administrativos disciplinares e congêneres, pois não lhe é permitida tal identificação).

d) Dados pessoais em assinaturas

Depreende-se que as assinaturas, sejam manuscritas ou eletrônicas, que contiverem dados pessoais disponibilizados pelo próprio titular, os respectivos dados, tal como o ato administrativo relacionado à respectiva assinatura são publicizáveis com o consentimento advindo do próprio ato da assinatura pelo titular de dados.

e) Dados pessoais em sistemas informatizados

Entende-se que as informações pessoais em sistemas informatizados que exigem controle mínimo de login, que se dá em função da unidade organizacional na qual o usuário esteja vinculado, e/ou perfil de usuário de funcionário/discente/externo, estão resguardadas em função das responsabilidades de cada usuário, que deverá:

I. guardar sigilo sobre fato ou informação de qualquer natureza de que tenha conhecimento por força de suas atribuições e/ou perfil, ressalvadas aquelas de acesso público;
II. comunicar aos gestores do sistema qualquer mudança percebida em privilégios de acesso ao Sistema.

6. BASE LEGAL DE SERVIÇOS, FINALIDADE E HIPÓTESE LEGAL DE TRATAMENTO DE DADOS PESSOAIS

Os serviços da Administração Pública são permeados por instrumentos legais externos e internos sem os quais não é possível se iniciar e concluir as atividades fins e meio da Universidade. Desta forma, toda ação, atividade ou serviço tem uma **base legal** que a define e, com isso, pressupõe-se que permita a captação e tratamento de dados pessoais para tal.

Assim, quanto ao tratamento de dados pessoais, que vai desde a captação desses dados ao arquivamento dos mesmos na instituição, este também tem sua **hipótese legal definida pela LGPD**, conforme o estabelecido nos artigos 7, que trata das hipóteses relacionadas aos dados pessoais, e 11, que trata das hipóteses de dados pessoais sensíveis:

- **Mediante o fornecimento de consentimento expresso pelo titular** (artigos 7, I, e 11, I da Lei nº 13.709/2018);
- **Cumprimento de obrigação legal ou regulatória pelo controlador** (artigos 7, II, e 11, II, a, da Lei nº 13.709/2018);
- **Execução de políticas públicas** (artigos 7, III, e 11, II, b, da Lei nº 13.709/2018);

- **Alguma espécie de estudo realizado por órgão de pesquisa** (artigos 7, IV, e 11, II, c, da Lei nº 13.709/2018);
- **Execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados** (artigos 7, V, e 11, II, d, da Lei nº 13.709/2018);
- **Exercício regular de direitos em processo judicial, administrativo ou arbitral** (artigo 7, VI, da Lei nº 13.709/2018);
- **Proteção da vida ou da incolumidade física do titular ou de terceiro** (artigos 7, VII, e 11, II, e, da Lei nº 13.709/2018);
- **Tutela da saúde** (artigos 7, VIII, e 11, II, f, da Lei nº 13.709/2018);
- **Atender aos interesses legítimos do controlador ou de terceiro** (artigo 7, XI, da Lei nº 13.709/2018);
- **Proteção do crédito** (artigo 7, X, Lei nº 13.709/2018);
- **Garantia da prevenção à fraude e à segurança do titular** (artigo 11, II, g, da Lei nº 13.709/2018).

Entretanto, é importante saber e prestar ciência da **finalidade específica** pela qual estamos realizando o respectivo tratamento de dados pessoais e dados pessoais sensíveis. Isto porque a LGPD deixa claro que se faz necessária uma mudança de cultura no que diz respeito à captação e todas as outras etapas de tratamento dos respectivos dados de uma pessoa natural e, sempre que possível, respeitando o direito à privacidade e à autodeterminação informativa, bem como outros fundamentos do artigo 2 da LGPD.

Desta forma, a instituição prioritariamente deverá realizar tratamento de dados pessoais apenas para o atendimento de finalidade específica, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público. Ou seja, não devem ser captados dados pessoais que não sejam necessários para os serviços prestados pela Universidade.

6.1. NOTIFICAÇÃO E TERMO DE CONSENTIMENTO

A Administração Pública, de maneira geral, **não precisa solicitar consentimento para titulares de dados pessoais e dados pessoais sensíveis**, conforme as hipóteses dos artigos 7º e 11 da LGPD. Porém, o interesse público deverá ser legítimo, demonstrando a finalidade específica e boa fé no tratamento de dados pessoais da política de privacidade da universidade.

Todas as unidades administrativas e acadêmicas da UNIRIO deverão ter conhecimento sobre a finalidade certa e a hipótese legal de todos os seus serviços e/ou atividades. Por isso, sugere-se, para o público externo, a elaboração de **termo ou aviso de notificação** nas atividades e/ou serviços ofertados pela Universidade, que informem o objetivo do tratamento de dados pessoais ou dados pessoais sensíveis e, sempre que possível, os seus respectivos instrumentos legais pertinentes, ou seja, a base legal que autoriza o tratamento de dados pessoais.

Observa-se que este termo ou aviso deverá vir destacado, sem a necessidade de caixa de seleção para documentos analógicos e com caixa de seleção de marcação obrigatória para formulários eletrônicos. Como por exemplo:

- Estou ciente de que **os dados pessoais** e/ou **os dados pessoais sensíveis** (discriminar o tipo de dados pessoais) aqui coletados se referem à(s) **atividade(s)** ou ao(s) **objetivo(s)** descrito(s) no próprio formulário (discriminar a atividade ou objetivo), cuja guarda do presente documento segue o que determinam os Códigos de Classificação de Documentos das Tabelas de Temporalidade e Destinação de Documentos de Atividade-Meio e Fim do Conarq.
- Estou ciente de que **os dados pessoais** e/ou **os dados pessoais sensíveis** (discriminar o tipo de dados pessoais) aqui coletados se referem à norma/legislação (especificar), cuja guarda será realizada pelo prazo prescricional, conforme as TTDD de Atividade-Fim e Meio do Conarq.
- Estou ciente de que **os dados pessoais** coletados no âmbito deste formulário para o presente evento estão sendo captados para **finalidade** (discriminar a finalidade) e que as imagens e som captadas serão divulgadas nas mídias sociais da instituição.
- Informa-se que **os dados pessoais** e/ou **os dados pessoais sensíveis** (discriminar o tipo de dados pessoais) aqui coletados se referem à finalidade (descrever), cuja guarda será realizada pelo prazo prescricional do respectivo documento/processo administrativo, conforme as TTDD de Atividade-Fim e Meio do Conarq.

Se cumpridos os requisitos acima descritos, tanto a população beneficiada toma ciência do início do tratamento de seus dados pessoais ou dados pessoais sensíveis, quanto os funcionários responsáveis pela coleta tomam conhecimento da sua responsabilidade no respectivo tratamento.

E nos casos em que as participações de titulares de dados pessoais ou dados pessoais sensíveis forem opcionais, como por exemplo, a participação eventual em uma ação promovida pela instituição sem produção de documentos comprobatórios de direitos ou deveres institucionais para com os participantes), os **termos de consentimento** para o tratamento de seus dados deverão conter a finalidade e o tempo de guarda discriminados, bem como a possibilidade de recusa do tratamento dos respectivos dados.

Em suma, para a padronização e em conformidade com os arts. 8, §1º, e 11, I, da LGPD, os termos de cientificação e de consentimento deverão estar destacados e conter as respectivas finalidades para o tratamento de dados pessoais ou dados pessoais sensíveis.

7. CONTRATAÇÃO DE SERVIÇOS E CONSTITUIÇÃO DE PARCERIAS

O tratamento de dados pessoais em contratos, termos, convênios ou instrumentos congêneres está respaldado pelo artigo 7, III e V, da LGPD.

O PARECER n. 00001/2024/CNCIC/CGU/AGU, que foi publicado por meio do Comunicado nº 08/2024 - Aplicabilidade da Lei Geral de Proteção de Dados (LGPD) aos

convênios e instrumentos congêneres, informa sobre a seguinte modificação nos respectivos instrumentos celebrados com a Administração Pública, que deverão ser atualizados:

- supressão de números de documentos de identificação pessoal, a exemplo de RG, carteira profissional e CPF, além de dados como estado civil e endereço residencial dos representantes dos partícipes nos convênios e instrumentos congêneres, bem como em atos de designação de fiscais.

Desta forma, as pessoas naturais serão identificadas por seus respectivos nomes, sendo que os representantes da Administração Pública poderão ser identificados nos respectivos instrumentos pelo nome, matrícula e portaria de nomeação/designação.

Assim, para os instrumentos anteriores, sugere-se o tarjamento de tais dados pessoais, com a garantia de guarda da sua reprodução fiel em outro meio por mesmo tempo do seu original, conforme as Tabelas de Temporalidade e Destinação de Documentos de Atividade-Meio e Fim do Conarq.

As partes entre si, por seus representantes, colaboradores e por quaisquer terceiros que por sua determinação participem da prestação de serviços objeto desta relação, comprometem-se a atuar de modo a proteger e a garantir o tratamento adequado dos dados pessoais a que tiverem acesso durante a relação contratual, bem como a cumprir as disposições da Lei nº 13.709/2018 (LGPD). Por isso, faz-se importante a pactuação, por meio de cláusulas, sobre as responsabilidades acerca da proteção e do tratamento de dados pessoais das partes que regem o contrato e que fizerem uso em razão da contratação.

Observa-se que as **parcerias estabelecidas com empresas ou instituições,** com ou sem efeitos financeiros, que operam os dados pessoais que a Universidade capta e trata, **devem constituir uma lista atualizada com o nome da entidade, objeto, finalidade, base e hipótese legal, duração de tratamento e descrição de dados pessoais sob tratamento.** Este controle é imprescindível para que a UNIRIO tenha sempre atualizada a listagem dos responsáveis pelo tratamento de seus dados pessoais.

Tais acordos e parcerias que fazem parte do ativo da Universidade têm que possuir cláusulas de **confidencialidade, termos de responsabilidade ou termos de sigilo no que tange ao tratamento de dados pessoais** geridos pelos operadores. Do mesmo modo, o tratamento de dados pessoais, a ser realizado pelos operadores constituídos em razão de parcerias e/ou contratações, não podem destoar da finalidade específica informada ao titular de dados pessoais na captação dos respectivos dados.

8. COMPARTILHAMENTO DE DADOS PESSOAIS

O compartilhamento de dados pessoais diz respeito a [início de citação] "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" [fim de citação] (ARTIGO 5, XVI, LGPD).

Neste escopo, a partilha de dados pessoais deverá ocorrer tendo em vista as hipóteses legais de tratamento de dados pessoais previstas pelos artigos 7 e 11 da LGPD, com a salvaguarda dos princípios gerais e da garantia dos direitos do titular prevista no artigo 6 da LGPD.

Desta forma, no compartilhamento de dados pessoais, deve-se assegurar a compatibilidade de finalidade de tratamento original informada ao titular, de forma que o tratamento realizado pelos operadores não divirja. Para tal, faz-se necessário que haja a formalização dos seguintes registros: discriminação do objeto, finalidade do tratamento, base e hipótese legal, duração do tratamento, e responsabilização acerca da proteção pelos dados pessoais compartilhados. Espera-se também a descrição de medidas de proteção de dados pessoais a serem adotadas pelos organismos com quem a instituição compartilha os respectivos dados pessoais.

Observa-se que, no compartilhamento de dados pessoais, também devem ser estabelecidos acordos de confidencialidade, termos de responsabilidade ou termos de sigilo com operadores, no que se relacione aos dados pessoais tratados pelos mesmos ou por terceirizações contratadas.

No caso de compartilhamento de dados com organizações internacionais, devem ser observados o que predispõem os artigos 33 e 34 da LGPD, sendo que a transferência internacional de dados pessoais deverá se limitar apenas ao necessário para o alcance das respectivas finalidades de seu tratamento.

Dessa forma, tanto para o compartilhamento nacional quanto internacional, a Universidade deverá manter uma lista atualizada com o nome da entidade, objeto, finalidade, base e hipótese legal, duração de tratamento, e descrição de dados pessoais compartilhados.

8.1. COMPARTILHAMENTO DE DADOS PESSOAIS POR ACERVOS INSTITUCIONAIS

O Arquivo Central e suas unidades de arquivo setoriais, em relação ao que dispõe a Resolução CONARQ n. 54, de 8 de dezembro de 2023, que versa sobre regras para a aplicação da normativa aos arquivos permanentes custodiados por pessoa física ou jurídica de direito público ou privado, utiliza para pesquisa no acervo o Termo de Responsabilidade (modelo anexo) que serve para pesquisas no acervo permanente e intermediário da Unirio.

Diante desse contexto normativo, o Arquivo Central considera de forma geral que, para os documentos sob sua custódia, sejam estes de guarda permanente ou intermediária, sendo de valor sócio-cultural e histórico que forem selecionados pelo corpo técnico da unidade:

- os dados pessoais de pessoas falecidas e consideradas ausentes judicialmente, não são sujeitos à LGPD;
- os dados pessoais não podem ser eliminados ou retificados sem a preservação dos estados documentais, a fim de garantir autenticidade e integridade dos documentos;
- os dados pessoais compartilhados com unidades da Unirio precisam possuir compatibilidade com a finalidade de tratamento original ou hipótese legal condizente com os artigos 7 e 11 da LGPD;
- os dados pessoais compartilhados com pesquisadores internos e externos devem ser viabilizados por meio de termo de responsabilidade e, nos seguintes casos, conforme a Resolução CONARQ n. 54/2018:

> I - prevenção e diagnóstico médico para utilização exclusivamente para tratamento dessa natureza;
> II - realização de estatísticas e pesquisas acadêmicas, científicas, genealógicas ou históricas;
> III - cumprimento de ordem judicial;
> IV - defesa de direitos humanos de terceiros; ou
> V - existência de interesse público geral e preponderante.

9. SEGURANÇA DO TRATAMENTO DE DADOS PESSOAIS

A segurança no tratamento de dados pessoais e dados pessoais sensíveis é um resultado do compromisso institucional na manutenção de suas atividades obrigatórias e regulatórias. Assim, depende de meios razoáveis e técnicos disponíveis para a garantia dos seus serviços, com transparência e baseada nos seguintes fundamentos:

> I - o respeito à privacidade;
> II - a autodeterminação informativa;
> III - a liberdade de expressão, de informação, de comunicação e de opinião;
> IV - a inviolabilidade da intimidade, da honra e da imagem;
> V - o desenvolvimento econômico e tecnológico e a inovação;
> VI - a livre iniciativa, à livre concorrência e à defesa do consumidor;
> VII - respeito aos direitos humanos, ao livre desenvolvimento da personalidade, à dignidade e ao exercício da cidadania pelas pessoas naturais (ARTIGO 2/LGPD).

Assim, para a garantia mínima de segurança dos dados pessoais e/ou dados pessoais sensíveis em meios analógicos ou digitais, a Universidade conta com um programa de gestão de documentos culturalmente estabelecido, que se baseia na aplicação do Plano de Classificação de Documentos de Arquivo (PDC) e o respectivo Código de Classificação de Documentos e Tabelas de Temporalidade e Destinação de Documentos (TTDD), relativos às Atividade-Meio e Atividade-Fim do Conselho Nacional

de Arquivos (Conarq). A observância da gestão arquivística sobre a documentação produzida e/ou recebida pela instituição é importante para a garantia dos prazos prescricionais dos respectivos documentos arquivísticos que contêm os dados pessoais e/ou dados pessoais sensíveis

Na manutenção e novas instalações de sistemas informatizados, recomenda-se a utilização dos guias disponibilizados pela Secretaria do Governo Digital (SGD),[3] cujo foco é a segurança dos respectivos sistemas, especialmente no que se relaciona aos dados pessoais e dados pessoais sensíveis. Além disso, faz-se importante a administração mínima de técnicas de segurança que remontam cinco princípios constantes na ABNT NBR ISO/IEC 27002: confiabilidade, integridade, disponibilidade, autenticidade e não-repúdio, ou irretratabilidade.

Além disso, as medidas de segurança adotadas para a proteção de dados na Universidade em sistemas informáticos deverão passar por periódica auditoria, a fim de avaliar as fragilidades dos respectivos sistemas. Contudo, sugere-se também a realização periódica do mapeamento de dados pessoais e dados pessoais sensíveis coletados no âmbito da Universidade, avaliação de vulnerabilidades e medidas corretivas, a fim de se evitar riscos à proteção dos respectivos dados.

De outra parte, uma estratégia importante estabelecida para a mitigação de vulnerabilidades no tratamento de dados pessoais e dados pessoais sensíveis são as capacitações internas, que vêm sendo ministradas desde 2010 e que versam sobre a gestão e classificação de documentos arquivísticos, a LAI e a LGPD, no âmbito da UNIRIO. Desta forma, faz-se necessária a continuidade da capacitação sobre a LGPD nos serviços oferecidos pela instituição e sua inserção ao plano de desenvolvimento de pessoal da UNIRIO.

9.1. MAPEAMENTO DE RISCOS E MITIGAÇÃO DE RISCOS

Faz parte do gerenciamento da segurança de dados pessoais e dados pessoais sensíveis o inventário dos riscos de manutenção de dados, independente do seu suporte. Por isso, o controlador e o operador de dados, bem como seus respectivos funcionários, deverão avaliar as rotinas de tratamento dos dados desde a coleta até a destinação final (arquivamento ou descarte, tendo em vista os Planos de Classificação de Documentos e Tabelas de Temporalidade e Destinação de Documentos para atividades meio e fim aprovadas pelo Conarq), a fim de realizar medidas corretivas no caso de riscos iminentes de divulgação não desejadas dos respectivos dados sob seu gerenciamento.

Desta forma, para a mitigação de riscos, podem ser implementadas as seguintes medidas:

- Compatibilidade do tratamento de dados pessoais à finalidade legítima para o respectivo tratamento;
- Controle de acesso ao local de armazenagem dos dados;

[3] Guias e modelos da SGD disponíveis em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias-e-modelos. Acesso em: 20 dez. 2023.

- Controle por perfil, login e a concessões de acessos em sistemas;
- Não fornecimento de informações a pessoas não autorizadas;
- Tarjamento de dados pessoais em publicização de documentos;
- Preenchimento de termos de responsabilidade quanto ao acesso à dados pessoais de outrem;
- Aplicação da gestão de documentos, tal como os prazos das Tabelas de Temporalidade e Destinação de Documentos, ou seja, os documentos são transferidos para a guarda de arquivos e a eliminação é feita por um Arquivista;
- Anonimização dos dados (quando o dado relativo a titular não pode ser identificado de nenhuma forma);
- Pseudonimização de dados (quando o dado perde a possibilidade de associação a um indivíduo, cuja associação ainda poderá ser feita em banco de dados complementar);
- Procedimentos regular de *backup*;
- Tratamento cíclico de riscos.

Observa-se que o tarjamento de dados pessoais[4] na publicização de documentos sempre deverá ocorrer quando o dado, combinado com outros, puder identificar uma pessoa natural, ou no caso que apenas o respectivo dado for capaz de validar campos de buscas.

9.2 PROCEDIMENTOS NO CASO DE INCIDENTES COM DADOS PESSOAIS

A partir do momento em que for constatado um incidente com dados pessoais sob tratamento da Universidade, todas as instâncias a ele relacionadas deverão ser comunicadas, incluindo a(o) Encarregada(o) pelo Tratamento de Dados Pessoais da UNIRIO, a fim de que a solução problema seja priorizado.

Assim, pontuamos os seguintes procedimentos:

I. **Comunicação** às instâncias competentes da Instituição relacionadas ao incidente;
II. **Solução do problema identificado**, conforme meios técnicos disponíveis, por quaisquer instâncias relacionadas ao incidente;
III. **Registro interno** do incidente com dados pessoais pela(o) Encarregada(o) pelo Tratamento de Dados Pessoais da UNIRIO;
IV. **Mitigação de riscos** relacionados ao incidente para que não se repita, conforme meios técnicos disponíveis;
V. **Comunicação à ANPD** pela UNIRIO, no caso de incidentes que possam acarretar risco ou dano relevante aos titulares, de acordo com o artigo 48 da LGPD.

[4] Para o tarjamento de número de CPF, com 11 dígitos recomenda-se que sejam tarjados os três primeiros dígitos e os três últimos: *****.XXX.XX*-****, bem como os demais números de identificação pessoal.

10. DECLARAÇÃO DE COOKIES

Os ***cookies*** são arquivos instalados no dispositivo que permitem a coleta de informações, ou seja, dados rastreáveis e, por isso, são dados que podem indiretamente identificar uma pessoa natural, por meio das informações coletadas.

Por padrão, a declaração de *cookies* em sítio eletrônico institucional deverá estar em destaque, em língua portuguesa, e permitir o seu gerenciamento mínimo, com a possibilidade de limitar tráfego e leitura do sítio eletrônico, com a rejeição total de todos os cookies não necessários. Desta forma, as opções deverão ser apresentadas de forma objetiva e não deverão vir assinaladas.

Assim, no ***banner* de declaração de *cookies*,** poderá ter opções como **desabilitar/rejeitar** todos os *cookies* não necessários, **habilitar/aceitar** todos os *cookies* e selecionar a habilitação de *cookies* específicos, sendo a última opção para os casos em que houver a necessidade de retenção de dados para funções específicas que deverão vir oportunamente descritas.

O *banner* de declaração de *cookies* também poderá conter link com as especificações sobre os dados retidos e o tempo de retenção dos dados, caso os mesmos não possam já estar explicitados nas próprias opções. E, para maior autonomia de usuários, faz-se importante informar como se pode realizar o bloqueio de *cookies* pelas configurações de navegadores mais frequentemente utilizados.

11. CASOS OMISSOS

Os casos não descritos e/ou dúvidas deverão ser demandados para a(o) Encarregada(o) pelo Tratamento de Dados Pessoais da UNIRIO, cujas informações estão fixadas no sítio eletrônico da instituição: https://www.UNIRIO.br/acessoinformacao/protecao-de-dados-pessoais, ou pelo endereço eletrônico específico lgpd@UNIRIO.br, conforme o artigo 41 da LGPD.

REFERÊNCIAS

ADVOCACIA-GERAL DA UNIÃO - AGU (Brasil). **Parecer n. 00002/2023/CNMLC/CGU/AGU.** Proteção da intimidade e sigilo de dados. Acesso em: 18 abr. 2024.

ADVOCACIA-GERAL DA UNIÃO - AGU (Brasil). **Parecer n. 00001/2024/CNCIC/CGU/AGU**. Aplicabilidade da Lei Geral de Proteção de Dados aos convênios e instrumentos congêneres. Acesso em: 18 abr. 2024.

Autoridade Nacional de Proteção de Dados - ANPD (Brasil). **Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado.** Brasília (DF): ANPD, 2022. Acesso em: 04 nov. 2023.

Autoridade Nacional de Proteção de Dados - ANPD (Brasil). **Guia orientativo Tratamento de dados pessoais para fins acadêmicos e para a realização de estudos e pesquisas.** Brasília (DF): ANPD, 2023. Acesso em: 04 nov. 2023.

Autoridade Nacional de Proteção de Dados - ANPD (Brasil). **Guia orientativo Cookies e proteção de dados pessoais.** Brasília (DF): ANPD, 2022. Acesso em: 02 jan. 2024.

Autoridade Nacional de Proteção de Dados - ANPD (Brasil). **Nota Técnica nº 85/2023/CGN/ANPD.** Sobre o conflito de entendimentos acerca do tratamento a ser conferido aos dados dos servidores públicos federais quanto à substituição do CPF dos servidores em contratos administrativos e outros documentos organizacionais pelo Siape e, em caso positivo, se deveria ser o Siape ocultado parcialmente para a publicação de tais atos ou contratos. Acesso em: 18 abr. 2024.

ARQUIVO NACIONAL (Brasil). **Dicionário brasileiro de terminologia arquivística.** Rio de Janeiro: Arquivo Nacional, 2005. Dicionário. Acesso em: 30 dez. 2023.

ARQUIVO NACIONAL (Brasil). **AN Digital: política de preservação digital.** Rio de Janeiro: Arquivo Nacional/MJSP, 2016. Acesso em: ago. 2022.

ARQUIVO NACIONAL (Brasil). **Gestão de documentos**: curso de capacitação para os integrantes do Sistema de Gestão de Documentos de Arquivo - SIGA, da administração pública federal. 2. edição. Rio de Janeiro: Arquivo Nacional, 2019. Acesso em: dez. 2022.

ARQUIVO NACIONAL (Brasil). **Código de classificação de documentos relativos às atividades-fim das instituições federais de ensino superior.** Acesso em: dez. 2022.

ARQUIVO NACIONAL (Brasil)**. Tabela de temporalidade de documentos relativos às atividades-fim das instituições federais de ensino superior.** Acesso em: dez. 2022.

ARQUIVO NACIONAL (Brasil). Resolução nº 54, de 8 de dezembro de 2023, que estabelece diretrizes e regras para a aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), aos arquivos permanentes custodiados por pessoa física ou jurídica de direito público ou privado. Acesso em: 10 jun. 2024.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **ABNT NBR ISO 27002:2013**: tecnologia da informação — técnicas de segurança — código de prática para controles de segurança da informação. Rio de Janeiro: ABNT, 2013.

BRASIL. **Lei nº. 12.527**, de 18 de novembro de 2011. Lei de Acesso à Informação. Acesso em: 10 dez. 2023.

BRASIL. **Lei nº. 13.709**, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Acesso em: 10 dez. 2023.

BRASIL. **Lei nº. 13.853**, de 8 de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Acesso em: 10 dez. 2023.

COMITÊ CENTRAL DE GOVERNANÇA DE DADOS (Brasil). **Guia de Boas Práticas para Implementação na Administração Pública Federal.** Brasília (DF): Comitê Central de Governança de Dados, 2020. Acesso em: 02 nov. 2023.

CONSELHO NACIONAL DE ARQUIVOS - Conarq (Brasil). **Resolução Conarq n. 20**, de 16 de julho de 2004. Dispõe sobre a inserção dos documentos digitais em programas de gestão arquivística de documentos dos órgãos e entidades integrantes do Sistema Nacional de Arquivos. Acesso em: 09 dez. 2020.

CONSELHO NACIONAL DE ARQUIVOS - Conarq (Brasil). **Resolução Conarq nº 43**, de 04 de setembro de 2015. Altera a redação da Resolução do Conarq nº 39, de 29 de abril de 2014, que estabelece diretrizes para a implementação de repositórios digitais confiáveis para a transferência e recolhimento de documentos arquivísticos digitais para instituições arquivísticas dos órgãos e entidades integrantes do Sistema Nacional de Arquivos (SINAR). Acesso em: ago. 2022.

CONSELHO NACIONAL DE ARQUIVOS - Conarq (Brasil). **Resolução Conarq nº 54**, de 8 de dezembro de 2023. Estabelece diretrizes e regras para a aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), aos arquivos permanentes custodiados por pessoa física ou jurídica de direito público ou privado. Acesso em: 03 jan. 2024.

SGD (Brasil). **Cartilha sobre finalidade e hipóteses legais.** Brasília (DF): Secretaria de Governo Digital, 2023. Acesso em: 05 jan. 2024.

MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS (MGI). Comunicado nº 08/2024 – Aplicabilidade da Lei Geral de Proteção de Dados (LGPD) aos convênios e instrumentos congêneres. Acesso em: 18 abr. 2024.

MINISTÉRIO DOS DIREITOS HUMANOS E DA CIDADANIA (Brasil). **Resolução nº 245, de 5 de abril de 2024.** Dispõe sobre os direitos das crianças e adolescentes em ambiente digital. Acesso em: 18 abr. 2024.

SILVA, Isabela Costa da; ABRANTES, Paula Cotrim de (Coordenação Técnica). Cartilha sobre a LGPD. Rio de Janeiro: Unirio, 2023. Acesso em: fev. 2024.

UNIVERSIDADE FEDERAL DO ESTADO DO RIO DE JANEIRO - UNIRIO (Brasil). **Sobre missão, visão e princípios**. Acesso em: 19 ago. 2022.

ANEXO - TERMO DE RESPONSABILIDADE (ARQUIVO CENTRAL)

TERMO DE RESPONSABILIDADE (CCD: 063.1)

Eu, _____,
CPF n. _____, residente na cidade _____, UF: _____, país: _____, telefone (_____)_____ ou correio eletrônico _____

Declaro ter concedido informações verdadeiras sobre mim e ter ciência de que é vedada a reprodução de quaisquer documentos do acervo do arquivo da Universidade Federal do Estado do Rio de Janeiro (UNIRIO) com finalidade comercial sem a autorização expressa da Universidade.

As reproduções que venham a ser publicadas sem finalidade comercial devem ser identificadas e informadas à UNIRIO, mantendo-se crédito institucional e de fonte.

Responsabilizo-me integralmente pela adequada utilização das informações a que tiver acesso; estou ciente de que posso vir a ser responsabilizado civil, criminal e administrativamente pelos danos morais ou materiais decorrentes da utilização, reprodução ou divulgação indevida dessas informações. Isento a administração pública federal, a Universidade Federal do Estado do Rio de Janeiro (UNIRIO) ou seus funcionários de qualquer responsabilidade a este respeito;

Declaro estar ciente do artigo 20 (divulgação autorizada ou necessária) da Lei n. 10.406/2002 (Código Civil) e os arts. 138 a 145 (crimes contra a honra), 297, 299 e 304 (crimes de falsidade documental) do Decreto-Lei n. 2.848/1940 (Código Penal).

Declaro estar ciente dos artigos 6, 14 e 25 da Lei de Arquivos n° 8.159 de 8 de janeiro de 1991, do Decreto n. 7.724/2012 (que regulamenta a Lei n° 12.527), da Lei de Acesso à Informação n° 12.527, artigo 31, referentes à violação de sigilo/ propriedade, desfiguração, destruição de documentos e das informações pessoais.

Declaro estar ciente do que prediz a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709, de 14 de agosto de 2018, atualizada pela Lei nº 13.853, de 8 de julho de 2019, no que tange à divulgação de dados pessoais sem

consentimento do titular dos dados para fins de pesquisa.

Autorizo a UNIRIO a ter acesso aos meus dados pessoais disponíveis neste Termo para controle de disponibilização de informações que possam também conter dados pessoais e para pesquisa de perfil de usuários de acervos arquivísticos.

Objetivo/Justificativa da pesquisa:

Rio de Janeiro, de de 202 .

Assinatura