POLÍTICA DE PRIVACIDADE E PROTEÇÃO DE DADOS

RECIFE-2024

FADE
UFPE

FOLHA DE CONTROLE

Informações Gerais

Título	Política de Privacidade e Proteção de Dados
Número de referência/Código	POL-SI-002
Status	Revisão
Autoria	Aurora Barros – Consultoria
Validação e Aprovação	Diretoria Executiva e Conselho de Curadores
Data da validação ou aprovação	Mai/2024
Validade	Indeterminada
Área Controladora da Política	Compliance

Histórico de Versões

Versão	**Motivo**	**Data**
1	Versão inicial	Mai/2024

FICHA TÉCNICA

Conselho de Curadores

Presidente do Conselho

Profª. Magdala de Araújo Novaes (Centro de Ciências Médicas – CCM)

Membros Titulares

Profª. Nadi Helena Presser (Centro de Artes e Comunicação – CAC)
Prof. Pablo Martin Rodriguez (Centro de Ciências Exatas e da Natureza – CCEN)
Profª. Sérgio Castelo Branco Soares (Centro de Informática – CIn)
Prof. Ricardo Pinto de Medeiros (Centro de Filosofia e Ciências Humanas – CFCH)
Profª. Darci Barbosa Lira de Melo (Centro de Educação – CE)
Prof. José Gilson de Almeida Teixeira Filho (Centro de Ciências Sociais e Aplicadas – CCSA)
Profª. Gabriela Cunha Schechtman Sette (Centro de Ciências da Saúde – CCS)
Prof. José Araújo dos Santos Júnior (Centro de Tecnologia e Geociências – CTG)
Prof. André Morgado Esteves (Centro de Biociências – CB)
Prof. Osmar Veras de Araújo (Centro Acadêmico do Agreste – CAA)
Profª. Lara Colognese Helegda (Centro Acadêmico de Vitória – CAV)
Prof. Humberto João Carneiro Filho (Centro de Ciências Jurídicas – CCJ)
Fernanda de Oliveira Muniz (Representante da Comunidade Estadual)

Membros Suplentes

Profª. Márcia Ivo Braz (Centro de Artes e Comunicação – CAC)
Prof. Eduardo Padrón Hernandéz (Centro de Ciências Exatas e da Natureza – CCEN)
Prof. André Luís de Medeiros Santos (Centro de Informática – CIn)
Prof. Reginaldo Gonçalves de Lima Neto (Centro de Ciências Médicas – CCM)
Prof. Francisco Jatobá de Andrade (Centro de Filosofia e Ciências Humanas – CFCH)
Prof. Ramon de Oliveira (Centro de Educação – CE)
Prof. Luiz Carlos Marques dos Anjos (Centro de Ciências Sociais e Aplicadas – CCSA)
Prof. Tony Meireles dos Santos (Centro de Ciências da Saúde – CCS)
Profª. Yêda Medeiros Bastos de Almeida (Centro de Tecnologia e Geociências – CTG)
Profª. Maria Teresa Jansem de Almeida Catanho (Centro de Biociências – CB)
Prof. Mário Rodrigues dos Anjos Neto (Centro Acadêmico do Agreste – CAA)
Prof. Emerson Peter da Silva Falcão (Centro Acadêmico de Vitória – CAV)

Política de Privacidade e Proteção de Dados

Equipe Fade-UFPE

Diretoria Executiva

Profª. Maira Galdino da Rocha Pitta, Diretora Presidente

Assessorias

Rosali Maria Oliveira de Albuquerque (Assessoria de Planejamento)
Ladice Albuquerque Marinho (Assessoria de Compliance e Controle Interno)
Anderson de Oliveira Vasconcelos (Assessoria de Inovação e Captação de Projetos)
Eduardo Pontes Barbosa (Assessoria de Tecnologia da Informação)
Raquel Souza Guimarães (Assessoria Jurídica)

Gerências

Iraci Pereira do Nascimento (Gerência de Recursos Humanos)
David Soares Pessoa (Gerência de Projetos 1)
Samia Amancio Sindeaux (Gerência de Projetos 2)
Danielle Anizia da Silva (Gerência de Projetos 3)
Suzan Kelly de Vasconcelos Siqueira (Gerência Administrativa e Financeira)

SUMÁRIO

COM A PALAVRA A ALTA DIREÇÃO

Na Fade-UFPE, nosso compromisso com a transparência, integridade e segurança dos dados pessoais de nossos colaboradores e parceiros é primordial. É com grande orgulho que apresentamos nossa política de privacidade e proteção de dados, refletindo nossos valores fundamentais e nosso compromisso com a com a cultura de compliance, proteção de dados e aplicação da Lei Geral de Proteção de Dados.

Vivemos em um mundo digital onde a proteção da privacidade e dos dados pessoais é uma responsabilidade compartilhada entre empresas e indivíduos. Nossa política define como coletamos, usamos, protegemos e compartilhamos informações pessoais em conformidade com as leis de privacidade de dados aplicáveis.

É essencial que todos nós, como membros desta organização, compreendamos e adotemos os princípios e diretrizes estabelecidos em nossa política. A proteção de dados não é apenas uma obrigação legal, mas também um reflexo de nosso compromisso com a confiança e o respeito aos direitos individuais.

Estamos comprometidos em manter nossos padrões de segurança e privacidade sempre atualizados, garantindo que os dados pessoais sejam tratados com cuidado e proteção. Continuaremos investindo em tecnologia e treinamento para garantir a conformidade contínua e aprimorar nossas práticas de proteção de dados.

Convido a todos a lerem atentamente nossa política de privacidade e proteção de dados e a nos contatar caso tenham alguma dúvida ou preocupação. Juntos, podemos garantir que a proteção de dados seja parte integrante de nossa cultura e práticas diárias.

Agradeço a todos por seu comprometimento contínuo com os padrões éticos e de segurança em tudo o que fazemos.

MAIRA GALDINO DA ROCHA PITTA:03997206422

Assinado de forma digital por MAIRA GALDINO DA ROCHA PITTA:03997206422
Dados: 2024.06.11 09:53:37 -03'00'

Profª. Maira Galdino da Rocha Pitta
Diretora Presidente da Fade-UFPE

Política de Privacidade e Proteção de Dados

1. INTRODUÇÃO

A importância da proteção de dados reside fundamentalmente na preservação da privacidade e segurança das informações pessoais, em um contexto global onde a digitalização e o processamento de dados tornam-se cada vez mais intrínsecos à vida cotidiana.

A proteção de dados pessoais não é apenas uma questão de cumprimento legal, mas, sobretudo, uma questão ética, que sustenta a confiança. A proteção eficaz dos dados pessoais ajuda a prevenir o abuso de informações, como fraudes, roubos de identidade e violações de privacidade, garantindo assim a integridade e a confidencialidade das informações pessoais.

Além disso, reforça o direito à privacidade, considerado fundamental em muitas sociedades, promovendo uma cultura de respeito e responsabilidade no tratamento de dados pessoais. Em última análise, a proteção de dados apoia a liberdade individual e a autodeterminação informativa, permitindo que as pessoas tenham controle sobre suas próprias informações em um mundo cada vez mais conectado e tecnológico.

2. OBJETIVO

O objetivo principal da política de privacidade e proteção de dados é garantir a segurança, privacidade e integridade das informações pessoais dos indivíduos, regulando a forma como os dados pessoais são coletados, processados, armazenados e compartilhados.

Esta política visa proteger os direitos fundamentais de liberdade e privacidade dos titulares, promovendo a transparência no uso de dados pessoais e estabelecendo regras claras para o tratamento dessas informações.

Além disso, busca-se fomentar a confiança entre os titulares e a nossa Fundação, incentivando a adoção de melhores práticas de segurança da informação e compliance legal, ao mesmo tempo em que se estabelecem mecanismos de responsabilização e penalidades para os casos de violações.

Em um mundo cada vez mais digitalizado, onde a quantidade de dados gerados e coletados cresce exponencialmente, a política de privacidade e proteção de dados torna-se essencial para salvaguardar a privacidade e os direitos individuais na era da informação.

3. A QUEM SE DESTINA

Todos que fazem parte da Fade-UFPE e que, direta e indiretamente, possam efetuar o tratamento de dados pessoais em nome da Fade-UFPE, não se limitando a:

- **Organizações Privadas:** Empresas de todos os tamanhos, desde startups até multinacionais, que coletam, processam ou armazenam dados pessoais como parte de suas operações;

- **Entidades Públicas:** Órgãos governamentais e instituições públicas que lidam com dados pessoais no curso de suas atividades, como a administração de serviços públicos, segurança e ordem pública;
- **Organizações Sem Fins Lucrativos:** Inclui ONGs, associações, fundações e qualquer outra entidade sem fins lucrativos que colete ou processe dados pessoais para alcançar seus objetivos;
- **Titulares dos Dados:** Indivíduos a quem os dados se referem, comumente conhecidos como "sujeitos dos dados". A política visa proteger seus direitos fundamentais e liberdades, especialmente no que diz respeito à sua privacidade e controle sobre seus dados pessoais;
- **Fornecedores de Serviços e Terceiros:** Parceiros, fornecedores, prestadores de serviços e qualquer terceiro que possa ter acesso a dados pessoais no contexto de serviços prestados a Fade-UFPE. Esses também estão sujeitos às obrigações de proteção de dados, especialmente no que se refere à segurança e à confidencialidade dos dados;
- **Autoridades Reguladoras:** Entidades governamentais ou independentes responsáveis por supervisionar a implementação e o cumprimento das leis de proteção de dados.

4. PRINCÍPIOS DA PROTEÇÃO DE DADOS

Além dos princípios identificados na Lei nº. 13.709/2018 (Lei Geral de Proteção de Dados), é imperioso destacar os princípios em que a Fade-UFPE está submetida, assim como todas as partes interessadas, acima identificadas. São eles:

- **Legalidade, Justiça e Transparência:** Os dados devem ser processados de maneira legal, justa e transparente em relação ao titular dos dados. Isso significa que as organizações devem ter uma base legal clara para processar dados pessoais e devem ser transparentes sobre como estes dados são usados;
- **Limitação da Finalidade:** Os dados pessoais devem ser coletados apenas para finalidades específicas, explícitas e legítimas, e não devem ser processados de maneira incompatível com essas finalidades. Qualquer uso posterior dos dados deve ser compatível com os propósitos originais para os quais foram coletados;
- **Minimização dos Dados:** Deve-se coletar apenas os dados pessoais que são estritamente necessários para os fins para os quais são processados. Isso significa que as informações coletadas devem ser adequadas, relevantes e limitadas ao necessário;
- **Exatidão:** Os dados pessoais devem ser precisos e, quando necessário, mantidos atualizados. Deve-se tomar todas as medidas razoáveis para garantir que os dados pessoais que são inexatos, considerando os fins para os quais são processados, sejam apagados ou retificados sem demora;
- **Limitação de Conservação:** Os dados pessoais devem ser mantidos em uma forma que permita a identificação dos titulares dos dados apenas pelo tempo necessário para os fins para os quais os dados pessoais são processados. Isso implica na implementação de políticas e medidas para garantir que os dados sejam apagados ou anonimizados quando não forem mais necessários;
- **Integridade e Confidencialidade (Segurança):** Os dados pessoais devem ser processados de uma maneira que garanta sua segurança, incluindo proteção contra

processamento não autorizado ou ilegal e contra perda, destruição ou dano acidental, usando medidas técnicas ou organizacionais adequadas;

- **Responsabilidade:** O controlador dos dados é responsável por, e deve ser capaz de demonstrar a conformidade com, os outros princípios de proteção de dados. Isso significa que as organizações devem não apenas cumprir estes princípios, mas também ser capazes de provar que estão cumprindo, por exemplo, através da implementação de políticas internas de proteção de dados, treinamento de funcionários e realização de auditorias regulares.

5. IDENTIFICAÇÃO E CLASSIFICAÇÃO DE DADOS PESSOAIS

A Lei Geral de Proteção de Dados (LGPD) do Brasil, estabelece um marco legal para a proteção de dados pessoais e impacta todas as organizações que processam dados de indivíduos no Brasil.

A LGPD classifica os dados pessoais em duas categorias principais: dados pessoais e dados pessoais sensíveis. A identificação e classificação desses dados são cruciais para a adequação e o cumprimento da lei.

5.1. DADOS PESSOAIS

São informações relacionadas à pessoa natural identificada ou identificável. Isso inclui uma ampla gama de informações que, direta ou indiretamente, podem identificar uma pessoa. Exemplos de dados pessoais incluem:

- Nome completo;
- Número de identidade (RG, CPF);
- Endereço de e-mail;
- Endereço residencial;
- Número de telefone;
- Informações de localização;
- Identificadores digitais (como endereços IP, cookies);
- Dados de comportamento e preferências pessoais.

5.2. DADOS PESSOAIS SENSÍVEIS

São um subconjunto de dados pessoais que estão relacionados a características específicas que podem ser utilizadas de forma discriminatória. A LGPD dá especial atenção a esses dados devido ao potencial risco de causar danos aos titulares dos dados. Exemplos de dados pessoais sensíveis incluem:

- Origem racial ou étnica;
- Convicção religiosa;
- Opinião política;
- Filiação a sindicato ou a Fundação de caráter religioso, filosófico ou político;
- Dados referentes à saúde ou à vida sexual;
- Dados genéticos ou biométricos, quando vinculados a uma pessoa natural.

A correta identificação e classificação dos dados pessoais e sensíveis são fundamentais para determinar o nível de proteção e as medidas de segurança necessárias. A LGPD exige que as organizações adotem procedimentos e práticas que garantam a proteção desses dados, com atenção especial aos dados sensíveis, que exigem consentimento específico e destacado para seu tratamento, exceto em casos previstos por lei.

6. TRATAMENTO DE DADOS PESSOAIS

A coleta e o tratamento de dados devem atender aos princípios acima postos e apresentados na LGPD e só pode ser realizada sob condições que garantam a proteção dos direitos fundamentais de liberdade e de privacidade.

O tratamento de dados é qualquer operação ou conjunto de operações realizadas com dados pessoais ou conjuntos de dados pessoais. Isso inclui desde a coleta inicial dos dados até sua eliminação final, abrangendo uma ampla gama de atividades que podem ser realizadas manualmente ou por meios automatizados.

Constitui tratamento de dados a sua coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

7. BASE LEGAL QUE FUNDAMENTA O TRATAMENTO DE DADOS

A LGPD estabelece que os dados pessoais só podem ser coletados nas seguintes circunstâncias:

- **Com o Consentimento do Titular dos Dados**: A base mais comum para a coleta de dados é o consentimento explícito e informado do titular dos dados. O consentimento deve ser fornecido de forma livre, informada e inequívoca, indicando concordância com o tratamento dos seus dados pessoais para uma finalidade específica;
- **Para o Cumprimento de Obrigação Legal ou Regulatória pelo Controlador**: Quando a coleta e o processamento de dados são necessários para que o controlador cumpra uma obrigação legal ou regulatória;
- **Para a Execução de Políticas Públicas**: Em casos específicos previstos em lei, para a execução de políticas públicas por parte da administração pública;
- **Para a Realização de Estudos por Órgão de Pesquisa**: Garantida, sempre que possível, a anonimização dos dados pessoais;
- **Para a Execução de Contrato ou de Procedimentos Preliminares Relacionados a Contrato**: Quando o tratamento de dados pessoais for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para procedimentos preliminares relacionados a um contrato;
- **Para o Exercício Regular de Direitos em Processo Judicial, Administrativo ou Arbitral**: Isso inclui a coleta de dados necessária para a defesa de direitos em processos de diversas naturezas;

- **Para a Proteção da Vida ou da Incolumidade Física do Titular dos Dados ou de Terceiro**: Em casos em que a coleta de dados é essencial para proteger a vida ou a segurança física do titular dos dados ou de outra pessoa;
- **Para a Tutela da Saúde**: Exclusivamente, em procedimento realizado por profissionais da área de saúde, serviços de saúde ou autoridade sanitária;
- **Para Atender aos Interesses Legítimos do Controlador ou de Terceiro**: Exceto nos casos em que os direitos e liberdades fundamentais do titular dos dados que requerem a proteção de dados pessoais prevaleçam;
- **Para a Proteção do Crédito**: Incluindo, conforme a legislação, o tratamento de dados necessário para a proteção do crédito.

8. DIREITOS DOS TITULARES DOS DADOS

A legislação vigente sobre proteção de dados estabelece uma série de direitos aos titulares dos dados pessoais, visando assegurar a proteção de suas informações e garantir o controle sobre seus próprios dados. Estes direitos são fundamentais para a promoção da transparência e para o fortalecimento da confiança entre titulares e entidades que tratam dados pessoais. Os principais direitos previstos na LGPD incluem:

- **Confirmação da Existência de Tratamento**: O titular tem o direito de obter a confirmação da existência de tratamento de seus dados pessoais;
- **Acesso aos Dados**: Os titulares podem acessar seus dados pessoais, obtendo cópias das informações que são tratadas pelas organizações;
- **Correção de Dados Incompletos, Inexatos ou Desatualizados**: Se os dados pessoais estiverem incompletos, inexatos ou desatualizados, o titular pode solicitar a correção ou complementação desses dados;
- **Anonimização, Bloqueio ou Eliminação de Dados Desnecessários, Excessivos ou Tratados em Desconformidade com a Lei**: Para dados que não estejam sendo tratados de acordo com a LGPD, o titular pode pedir sua anonimização, bloqueio ou eliminação;
- **Portabilidade dos Dados**: O titular dos dados tem o direito de solicitar a portabilidade de seus dados pessoais a outro fornecedor de serviço ou produto, respeitados os segredos comercial e industrial, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional;
- **Eliminação dos Dados Tratados com o Consentimento do Titular**: Exceto em casos onde a lei oferece outras bases legais para o tratamento de dados, o titular pode solicitar a eliminação dos dados pessoais tratados com base em seu consentimento;
- **Informação das Entidades Públicas e Privadas com as Quais o Controlador Realizou Uso Compartilhado de Dados:** O titular pode solicitar informações sobre com quais entidades o controlador compartilhou seus dados;
- **Informação sobre a Possibilidade de Não Fornecer Consentimento e sobre as Consequências da Negativa**: Os titulares têm o direito de ser informados sobre as consequências de não fornecerem seu consentimento para o tratamento de seus dados pessoais;

- **Revogação do Consentimento**: O titular pode revogar seu consentimento a qualquer momento, por procedimento gratuito e facilitado, sendo os dados então obrigatoriamente eliminados, exceto em casos previstos em lei.

Esses direitos podem ser exercidos pelos titulares e a Fade-UFPE se valerá de todos os esforços e meios adequados e efetivos para que os titulares possam exercê-los.

9. COMPARTILHAMENTO DE DADOS COM TERCEIROS

O compartilhamento de dados deve respeitar os princípios da finalidade, adequação, necessidade, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas. Isso significa que qualquer compartilhamento de dados deve ter uma finalidade legítima, específica e informada ao titular, além de ser compatível com as finalidades originais para as quais os dados foram coletados.

9.1. CONDIÇÕES PARA O COMPARTILHAMENTO DE DADOS

A LGPD estabelece que o compartilhamento de dados pessoais deve ocorrer em situações específicas e sob condições claras:

- **Com Consentimento do Titular**: O compartilhamento pode ocorrer com o consentimento explícito do titular dos dados, que deve ser informado sobre com quem os dados serão compartilhados e para quais finalidades;
- **Sem Consentimento do Titular**: Em certas condições, o compartilhamento pode ocorrer sem o consentimento do titular, como para o cumprimento de uma obrigação legal, para a execução de políticas públicas, para a realização de estudos por órgão de pesquisa, para a proteção da vida ou da incolumidade física do titular ou de terceiros, para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias, ou para a proteção do crédito.

9.2. TRANSPARÊNCIA E DIREITOS DOS TITULARES

A transparência é um pilar fundamental, exigindo que os titulares dos dados sejam informados sobre o compartilhamento de seus dados, incluindo as entidades com as quais os dados são compartilhados e os propósitos específicos do compartilhamento. Além disso, os titulares têm o direito de acessar informações sobre o compartilhamento de seus dados e podem exercer outros direitos previstos na LGPD, como a correção de dados incompletos, inexatos ou desatualizados.

9.3. MEDIDAS DE SEGURANÇA

As organizações envolvidas no compartilhamento de dados devem adotar medidas de segurança, técnicas e administrativas adequadas para 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.

9.4. RESPONSABILIDADE E PRESTAÇÃO DE CONTAS

Organizações que tratam dados pessoais devem não apenas cumprir com as obrigações estabelecidas pela LGPD, mas também demonstrar a qualquer momento que estão fazendo isso, adotando práticas e políticas que assegurem a conformidade com a lei, incluindo no contexto de compartilhamento de dados.

10. SEGURANÇA DOS DADOS

A segurança de dados é um aspecto crítico da gestão de informações na era digital, envolvendo a implementação de medidas técnicas, físicas e administrativas para proteger dados pessoais e corporativos contra acessos não autorizados, perdas, alterações indevidas, divulgação, destruição ou qualquer outra forma de tratamento inseguro.

Essas medidas incluem, mas não se limitam a criptografia, controle de acesso, avaliações de vulnerabilidade, treinamentos de conscientização em segurança para funcionários, backups regulares e planos de resposta a incidentes. A segurança de dados não apenas salvaguarda as informações importantes das organizações e indivíduos contra ameaças cibernéticas, mas também assegura a conformidade com regulamentações de proteção de dados, como a GDPR na União Europeia e a LGPD no Brasil, fortalecendo a confiança das partes interessadas e mantendo a integridade e a reputação das entidades envolvidas. Devendo sempre ser observada a POLÍTICA DE SEGURANÇA DA INFORMAÇÃO e demais PROCEDIMENTOS relacionados ao tema.

11. VIOLAÇÃO DE DADOS

A LGPD enfatiza a importância da adoção de medidas preventivas, mas também reconhece que violações podem ocorrer e, quando isso acontece, é crucial ter um plano de resposta bem definido. Os procedimentos a serem seguidos incluem:

- **Detecção e Avaliação do Incidente**: Imediatamente após a identificação de uma violação de dados, a Fade-UFPE deve avaliar a extensão e a gravidade do incidente, determinando quais dados foram afetados e qual o potencial impacto para os titulares dos dados;
- **Contenção e Mitigação**: Devem ser tomadas medidas imediatas para conter a violação e mitigar seus efeitos. Isso pode incluir a suspensão de sistemas específicos, a alteração de senhas ou o isolamento de partes da rede;
- **Notificação às Autoridades**: A LGPD exige que a Autoridade Nacional de Proteção de Dados (ANPD) seja notificada em um prazo razoável, que, conforme a regulamentação, é de até dois dias úteis, dependendo da gravidade do incidente e do risco ou dano aos titulares dos dados;
- **Comunicação aos Titulares dos Dados**: Além de notificar a ANPD, a Fade-UFPE deve comunicar o incidente de forma clara e adequada aos titulares dos dados afetados, especialmente se o incidente representar um risco elevado aos seus direitos e liberdades. A comunicação deve incluir informações sobre a natureza do incidente, os dados afetados,

os possíveis impactos, as medidas que estão sendo tomadas para resolver a situação e como os titulares podem se proteger;

- **Documentação e Avaliação**: Todo o processo de resposta ao incidente deve ser documentado, incluindo as decisões tomadas e as ações realizadas. Após a resolução do incidente, é recomendável realizar uma avaliação pós-incidente para identificar as causas, avaliar a eficácia das medidas de resposta e ajustar os planos de segurança e resposta a incidentes conforme necessário;
- **Melhoria Contínua**: a Fade-UFPE utilizará as lições aprendidas com o incidente para melhorar continuamente as políticas e práticas de segurança de dados, ajustando os controles de segurança para prevenir futuras violações.

Estabelecer e seguir esses procedimentos não apenas cumpre com as exigências da LGPD, mas também demonstra o compromisso Fade-UFPE com a proteção de dados pessoais, contribuindo para a confiança do titular e o compliance.

12. TRANSFERÊNCIAS INTERNACIONAIS DE DADOS

As Transferências Internacionais de Dados sob a Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, são permitidas, mas estão sujeitas a condições específicas para assegurar que o nível de proteção de dados pessoais não seja comprometido quando esses são transferidos para fora do Brasil. A LGPD estabelece uma série de mecanismos e garantias que devem ser observados para que tais transferências sejam realizadas de forma legal e segura:

- **Adequação de Proteção de Dados**: A transferência pode ocorrer para países ou organismos internacionais que proporcionem um grau de proteção de dados pessoais adequado ao previsto na LGPD. A Autoridade Nacional de Proteção de Dados (ANPD) é responsável por avaliar e declarar a adequação desses níveis de proteção;
- **Garantias Contratuais**: Na ausência de uma decisão de adequação, a transferência internacional de dados pode ser realizada mediante a oferta de garantias suficientes de proteção, por meio de cláusulas contratuais específicas para a situação, cláusulas contratuais padrão, normas corporativas globais ou selos, certificados e códigos de conduta aprovados;
- **Consentimento Específico**: A transferência pode ocorrer com o consentimento específico e destacado do titular dos dados, após ser informado sobre as condições internacionais da transferência, a natureza dos dados a serem transferidos e os riscos envolvidos;
- **Cumprimento Legal e Proteção do Titular**: A LGPD também permite a transferência de dados para a proteção do crédito, bem como para o cumprimento de obrigação legal ou regulatória pelo controlador, para a execução de políticas públicas ou atribuição legal do serviço público, para a realização de estudos por órgão de pesquisa, para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido desse, ou para o exercício regular de direitos em processo judicial, administrativo ou arbitral;
- **Cooperação Internacional**: A transferência de dados pode ser necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, investigação e fiscalização, conforme os meios legais previstos em acordos internacionais.

A LGPD estabelece que qualquer transferência internacional de dados deve garantir que os dados pessoais estejam sujeitos a um regime de proteção compatível com a legislação brasileira. Além disso, a ANPD pode estabelecer normas complementares sobre as condições de transferência de dados, incluindo a verificação de requisitos específicos para determinados países ou setores. As organizações devem, portanto, avaliar cuidadosamente as condições sob as quais realizam transferências internacionais de dados, assegurando a conformidade com a LGPD e protegendo os direitos dos titulares dos dados.

13. AGENTES DE TRATAMENTO DE DADOS

Os agentes de proteção de dados são categorizados principalmente em dois grupos: o controlador e o operador. Além disso, a figura do encarregado de proteção de dados (DPO - Data Protection Officer) também desempenha um papel crucial no ecossistema de proteção de dados. Cada um desses agentes tem responsabilidades específicas no tratamento de dados pessoais:

- **Controlador**: É a pessoa natural ou jurídica, de direito público ou privado, que tem competências para tomar as decisões referentes ao tratamento de dados pessoais. O controlador é responsável por determinar as finalidades e os meios pelos quais os dados pessoais são processados. Isso inclui decidir sobre quais dados serão coletados, a finalidade da coleta e como os dados serão utilizados. O controlador tem a responsabilidade principal de garantir a conformidade com a LGPD, incluindo a proteção dos direitos dos titulares dos dados;
- **Operador**: É a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. O operador atua sob as ordens do controlador, seguindo suas instruções para processar os dados pessoais para os fins determinados por aquele. Embora o operador não tome as decisões sobre os aspectos principais do tratamento de dados (como finalidade e meios), ele tem a responsabilidade de garantir a segurança dos dados durante o processamento e de seguir as diretrizes estabelecidas pelo controlador;
- **Encarregado de Proteção de Dados (Data Protection Officer - DPO)**: O DPO é a pessoa indicada pelo controlador e pelo operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). O DPO tem várias responsabilidades, incluindo o monitoramento da conformidade da Fundação com a LGPD, a orientação de funcionários, estagiários, e prestadores de serviço acerca das práticas de proteção de dados, a realização de auditorias periódicas para assegurar a conformidade, e o atendimento às solicitações dos titulares dos dados e da ANPD. Embora a LGPD especifique situações em que a nomeação de um DPO é obrigatória, qualquer Fundação pode se beneficiar da nomeação de um DPO para gerenciar suas obrigações de proteção de dados.

Estes agentes desempenham papéis fundamentais no ecossistema de proteção de dados, trabalhando juntos para garantir que o tratamento de dados pessoais seja realizado de forma segura, transparente e conforme as disposições legais estabelecidas pela LGPD.

14. TREINAMENTO E CONSCIENTIZAÇÃO

O treinamento e a conscientização sobre a política de privacidade e proteção de dados são componentes essenciais para garantir a conformidade com leis como a Lei Geral de Proteção de Dados (LGPD) no Brasil e outras regulamentações semelhantes ao redor do mundo. Essas atividades visam educar os colaboradores e parceiros sobre a importância da proteção de dados, os princípios fundamentais da LGPD, os direitos dos titulares dos dados, e as responsabilidades dos agentes de tratamento (controladores e operadores). A seguir, detalhamos os aspectos cruciais desses processos de treinamento e conscientização.

14.1. OBJETIVOS DO TREINAMENTO E CONSCIENTIZAÇÃO

Compreender a Importância da Proteção de Dados: Sensibilizar todos os envolvidos sobre a importância de proteger os dados pessoais, destacando as consequências legais, financeiras e de reputação em caso de não conformidade.

- **Conhecimento da Legislação**: Proporcionar um entendimento claro da LGPD e de outras leis aplicáveis, incluindo os princípios de tratamento de dados, as categorias de dados protegidos, e as obrigações legais;
- **Práticas Seguras de Tratamento de Dados**: Instruir sobre as melhores práticas e procedimentos seguros para o tratamento de dados, incluindo coleta, armazenamento, processamento e eliminação de dados pessoais;
- **Gestão de Incidentes**: Ensinar como identificar, reportar e responder a potenciais incidentes de segurança de dados, incluindo violações de dados pessoais.

14.2. ESTRATÉGIAS DE IMPLEMENTAÇÃO

Programas de Treinamento Personalizados: Desenvolver programas de treinamento que sejam relevantes para diferentes níveis da Fundação, desde a alta gestão até os operacionais, adaptando o conteúdo às suas funções específicas.

- **Uso de Diversos Métodos de Ensino**: Aplicar uma variedade de métodos de ensino, como workshops, seminários, e-learning, vídeos educativos e quizzes para reforçar o aprendizado;
- **Material de Apoio**: Disponibilizar manuais, políticas, procedimentos e FAQs que possam ser consultados a qualquer momento para esclarecer dúvidas sobre a proteção de dados;
- **Atualizações Regulares**: Garantir que o treinamento seja atualizado regularmente para refletir quaisquer mudanças na legislação, na política interna de proteção de dados ou no ambiente tecnológico;
- **Avaliações e Feedback**: Realizar avaliações periódicas para medir o entendimento e a aplicação dos conhecimentos adquiridos, além de coletar feedback para melhorar continuamente os programas de treinamento.

Criar uma cultura de proteção de dados na Fundação é fundamental. Isso não se limita a realizar treinamentos obrigatórios; envolve criar uma mentalidade onde a proteção de dados seja uma prioridade em todos os níveis. A conscientização contínua e o engajamento ativo dos colaboradores são cruciais para esse processo. A proteção de dados deve ser vista como um valor da empresa, e não apenas como uma obrigação legal.

Implementar um programa eficaz de treinamento e conscientização sobre a política de privacidade e proteção de dados não apenas ajuda a minimizar os riscos de não conformidade e violações de dados, mas também reforça a confiança das pessoas que se relacionam com a Fundação em sua capacidade de proteger informações sensíveis.

15. AUDITORIA E MONITORAMENTO

A auditoria em relação à LGPD envolve a revisão sistemática das práticas, políticas e procedimentos relacionados ao tratamento de dados pessoais dentro de uma Fundação. O objetivo é verificar a conformidade com a lei, identificar lacunas e riscos, e recomendar melhorias. Isso pode incluir, mas não se limita a:

a. Avaliação da adequação das políticas de privacidade e proteção de dados.
b. Verificação da existência e eficácia das medidas de segurança da informação.
c. Análise da legalidade, transparência e finalidade na coleta e uso dos dados.
d. Revisão dos processos de consentimento e das práticas de governança de dados.
e. Exame dos contratos com operadores e parceiros terceirizados, assegurando que esses também estejam em conformidade.

O monitoramento contínuo é crucial para a detecção precoce de qualquer desvio ou não conformidade com a LGPD. Isso pode ser realizado por meio de sistemas automatizados e procedimentos regulares que incluem:

a. Acompanhamento constante das operações de tratamento de dados para assegurar que sejam executadas conforme as políticas estabelecidas;
b. Implementação de sistemas de gestão de incidentes para garantir respostas rápidas e eficazes a qualquer violação de dados;
c. Realização de análises de risco e avaliações de impacto à proteção de dados (DPIA - Data Protection Impact Assessment) para novos projetos ou mudanças significativas nas operações;
d. Monitoramento da eficácia das medidas técnicas e organizacionais de segurança de dados.

A auditoria e o monitoramento não são apenas requisitos legais, mas também práticas essenciais para a gestão de riscos, fortalecendo a confiança dos titulares dos dados e promovendo uma cultura de transparência e responsabilidade na proteção de dados pessoais.

16. ATUALIZAÇÕES DA POLÍTICA

Esta política deverá receber atualizações periódicas sob os seguintes critérios:

- **Revisão Anual**: Realizar uma revisão anual como prática padrão, mesmo na ausência de mudanças significativas, para garantir que a política permaneça relevante e atualizada;
- **Após Mudança Significativa nas Operações ou na Legislação**: Sempre que houver mudança significativa nas operações de negócios, nas tecnologias de processamento de

dados, ou nas leis e regulamentações aplicáveis, é crucial revisar e, se necessário, atualizar a política de privacidade e proteção de dados para refletir essa mudança;

- **Em Resposta a Incidente de Segurança**: Após um incidente de segurança de dados, é importante revisar a política para identificar quaisquer lacunas ou deficiências que possam ter contribuído para o incidente e atualizá-la para prevenir futuras ocorrências.

17. MEDIDAS DISCIPLINARES

17.1. MEDIDAS DISCIPLINARES EXTERNAS

No contexto da LGPD e de políticas internas de empresas, as medidas disciplinares podem abranger tanto sanções legais aplicadas por autoridades reguladoras quanto consequências internas definidas pela Fundação. Aqui estão alguns exemplos:

- **Sanções Legais**: LGPD e Outras Legislações de Proteção de Dados;
- **Multa**: A LGPD estabelece que as multas por descumprimento podem chegar a 2% do faturamento da empresa no Brasil, limitado a R$ 50 milhões por infração;
- **Advertência**: Com indicação de prazo para adoção de medidas corretivas;
- **Publicização da Infração**: Após devidamente apurada e confirmada a infração, a autoridade pode ordenar a divulgação do fato;
- **Bloqueio dos Dados Pessoais**: Até a regularização da situação que causou a infração;
- **Eliminação dos Dados Pessoais**: Relacionados à infração.

17.2. MEDIDAS DISCIPLINARES INTERNAS

- **Advertência Verbal ou Escrita**: Para infrações leves ou como primeira medida;
- **Suspensão**: Temporária das atividades do colaborador, sem remuneração, como forma de penalidade por infrações mais graves;
- **Treinamento ou Reciclagem Obrigatória**: Para reforçar a importância das políticas de proteção de dados e evitar reincidências;
- **Demissão por Justa Causa**: Para casos de descumprimento grave e intencional das políticas de proteção de dados, que coloquem em risco significativo a segurança das informações ou violem direitos de titulares de dados;
- **Ações Legais**: A Fundação pode tomar medidas legais contra o colaborador, buscando reparação por danos causados à empresa devido ao descumprimento das políticas de proteção de dados.