CARTILHA

LGPD

Compliance e Integridade



FINDES
SESI | SENAI | IEL | CINDES

Sumário

1. Introdução
2. Objetivo
3. Recados do Comitê
4. Entendendo a LGPD e seus princípios
5. Pilares da Segurança da Informação
6. Definições Legais: Dados Pessoais e Dados Sensíveis
7. Quem são os protagonistas no tratamento de dados?
8. Papéis e responsabilidades na FINDES
9. Tratamento de dados de crianças e adolescentes
10. Direito dos titulares e o ciclo de vida dos dados
11. Boa prática no uso de documentos
12. Boas práticas no dia a dia
13. Utilização de aplicativos, sistemas e equipamentos
14. Uso de dados pessoais em Inteligência Artificial
15. Procedimentos em casos de incidentes e consequências
16. Participação em treinamentos
17. Canais de comunicação e suporte
18. Glossário
19. Referências e recursos adicionais

1. Introdução

O QUE É IMPORTANTE, A GENTE CUIDA.

Bem-vindo(a) ao nosso Guia Integrado de Proteção de Dados.
A proteção de dados pessoais é essencial para garantir a privacidade, a segurança e a confiança nas relações. Esta cartilha apresenta, de forma simples e prática, os principais conceitos da LGPD e as boas práticas que devem fazer parte da rotina de todos.

Ao seguir estas orientações, você contribui para um ambiente mais seguro, transparente e em conformidade com a legislação, fortalecendo a relação de confiança com nossos clientes, parceiros, alunos e colaboradores.

2. Objetivo

Este manual visa orientar os usuários sobre boas práticas, condutas esperadas e responsabilidades no uso de recursos tecnológicos, assegurando a confidencialidade, a integridade e a disponibilidade das informações, bem como o cumprimento das normas legais e regulatórias aplicáveis, como a Lei Geral de Proteção de Dados Pessoais (LGPD).

3. Recados do Comitê de Dados, Privacidade e Segurança da Informação

A privacidade, a proteção de dados e a segurança da informação são compromissos de todos nós e fundamentais para uma organização ética, segura e responsável.

Acreditamos que **conscientizar, orientar e capacitar são as melhores formas de prevenir riscos e fortalecer uma cultura de proteção de dados.** Por isso, este guia foi desenvolvido para apoiar nossos colaboradores na compreensão e aplicação dos princípios da LGPD em suas atividades diárias.

Mais do que cumprir a legislação, proteger dados significa respeitar as pessoas, suas informações e a confiança depositada em nossa organização.
O Comitê de Privacidade, Dados e Segurança da Informação está à disposição para apoiar essa jornada. **Privacidade e segurança são responsabilidades de todos e devem fazer parte das nossas decisões todos os dias.**

Comitê de Privacidade, Dados e Segurança da Informação.

4. Entendendo a LGPD e seus princípios

POR QUE A PROTEÇÃO DE DADOS É TÃO IMPORTANTE HOJE?

A LGPD existe para garantir que os direitos básicos de cada pessoa, como a privacidade, sejam respeitados. Em tempos de crescente uso de ferramentas tecnológicas, estamos mais suscetíveis a riscos de ciberataques e vazamentos de dados.

Um exemplo marcante foi o vazamento de dados conhecido como "RockYou2021", em que foram disponibilizados na internet cerca de 8,4 bilhões de senhas de usuários de vários países. Este evento realça os enormes riscos associados ao armazenamento de dados e a necessidade crítica de protegê-los adequadamente.

O QUE É A LGPD?

A Lei Geral de Proteção de Dados Pessoais (LGPD) é a legislação brasileira que cria as regras para o uso de dados pessoais por empresas e órgãos públicos, tanto em meios físicos (papel) como digitais.

QUEM DEVE CUMPRIR A LEI?

A LGPD aplica-se ao tratamento de dados pessoais realizado por pessoas naturais ou por pessoas jurídicas de direito público ou privado, nos meios físicos ou digitais, nas hipóteses previstas em lei.

A LGPD prevê situações específicas em que suas regras não se aplicam, como determinados tratamentos realizados por pessoa natural para fins exclusivamente particulares e não econômicos, bem como para fins exclusivamente jornalísticos, artísticos ou acadêmicos, entre outras hipóteses legais.

OS 10 PRINCIPIOS DA LGPD:

Finalidade: Uso para propósitos legítimos, específicos e informados ao titular.
Adequação: Compatibilidade do tratamento com as finalidades informadas.
Necessidade: Coleta limitada ao mínimo necessário para a finalidade.
Livre acesso: Garantia de consulta facilitada sobre a forma e duração do tratamento.
Qualidade dos dados: Exatidão, clareza e atualização dos dados.

Transparência: Informações claras e acessíveis sobre o tratamento.
Segurança: Medidas técnicas e administrativas de proteção.
Prevenção: Adoção de medidas para prevenir danos.
Não discriminação: Vedação ao tratamento para fins discriminatórios.
Responsabilização e prestação de contas: Comprovação da adoção de medidas eficazes.

ÉTICA NO USO DE DADOS

Ao usar um dado pessoal, devemos ter em mente que aquela informação nos foi confiada. É fundamental agir de forma correta, usando o dado apenas para o fim combinado e garantindo que ele esteja seguro.

5. Pilares da segurança da informação

Enquanto a LGPD trata dos princípios que legitimam o uso de dados pessoais, a Segurança da Informação trata de como esses dados (e todas as demais informações da FINDES) são protegidos tecnicamente. Os dois conjuntos de princípios se complementam.

CONFIDENCIALIDADE

Garantir que as informações sejam acessadas apenas por pessoas devidamente autorizadas, prevenindo vazamentos, acessos indevidos ou não intencionais.

INTEGRIDADE

Assegurar que as informações permaneçam íntegras, precisas e confiáveis ao longo de seu ciclo de vida, evitando alterações não autorizadas ou acidentais.

DISPONIBILIDADE

Garantir que as informações e os sistemas estejam acessíveis e operacionais sempre que necessários para o desempenho das atividades institucionais.

Todos os documentos e informações produzidos no exercício da função são de propriedade da FINDES. Quem tiver acesso a informações, confidenciais ou não, deve manter o sigilo, inclusive após o término do vínculo com a instituição.

6. Definições legais: Dados pessoais e dados sensíveis

DADOS PESSOAIS

São dados pessoais que, por sua natureza, demandam proteção especial, como aqueles relacionados à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, saúde, vida sexual e dados genéticos ou biométricos, quando vinculados a uma pessoa natural.

DADOS PESSOAIS SENSÍVEIS

São dados mais íntimos e que, por isso, precisam de um cuidado redobrado. Falam sobre origem racial ou étnica, religião, opiniões políticas, filiação a sindicatos, saúde, vida sexual, dado genético ou biométrico.

Exemplos de documentos que podem conter dados sensíveis: atestados médicos, fichas de saúde de alunos, atestado de Saúde Ocupacional (ASO), entre outros.

COMO DADOS SENSÍVEIS SÃO TRATADOS?

O tratamento de dados pessoais sensíveis somente pode ocorrer nas hipóteses previstas no art. 11 da LGPD, que incluem o consentimento específico e destacado do titular e outras bases legais.

Entretanto, poderá ser tratado sem consentimento quando indispensável para:

- Cumprimento de obrigação legal ou regulatória pelo controlador;
- Tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
- Realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados sensíveis;
- Exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral;
- Proteção da vida ou da segurança física do titular ou de terceiros;
- Tutela da saúde;
- Garantia da prevenção à fraude e à segurança do titular.

DADOS ANONIMIZADOS

São dados que, mediante a utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, não permitem identificar o titular. Em regra, dados efetivamente anonimizados não são considerados dados pessoais para fins da LGPD, salvo quando o processo de anonimização puder ser revertido nas condições previstas em lei.

7. Quem são os protagonistas no tratamento de dados?

TITULAR

É a pessoa natural a quem os dados pessoais se referem. Por exemplo: você, um colaborador, aluno, cliente ou outro indivíduo cujas informações sejam tratadas pela FINDES.

CONTROLADOR

Pessoa natural ou jurídica responsável pelas principais decisões referentes ao tratamento de dados pessoais.

OPERADOR

Pessoa natural ou jurídica que realiza o tratamento de dados pessoais em nome do controlador e conforme suas instruções.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

É a autoridade responsável por zelar pela proteção de dados pessoais e por regulamentar, orientar e fiscalizar o cumprimento da LGPD, no âmbito de suas competências.

8. Papéis e responsabilidades na FINDES

COLABORADORES

- Utilizar dados pessoais apenas para as finalidades autorizadas pela função exercida;
- Seguir as políticas internas de segurança da informação e privacidade;
- Comunicar imediatamente qualquer incidente, suspeita ou dúvida ao Encarregado de Dados (DPO);
- Participar dos treinamentos e capacitações oferecidos.

GESTORES E LIDERANÇAS

- Garantir que sua área/equipe cumpra a LGPD e as políticas internas;
- Autorizar acessos a dados pessoais de forma criteriosa (princípio da necessidade);
- Disseminar a cultura de proteção de dados junto às equipes;
- Reportar ao Comitê de Dados, Privacidade e segurança da informação riscos identificados em seus processos;

COMITÊ DE DADOS, PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

Instituído por Portaria da Presidência da FINDES, é responsável por propor ações de comunicação e capacitação, oferecer parecer sobre incidentes de segurança que envolvam dados pessoais e supervisionar o cumprimento de normas e políticas de segurança e privacidade de dados.

ENCARREGADO DE DADOS (DPO)

O Encarregado de Dados Pessoais (DPO) atua como canal de comunicação entre a FINDES, os titulares e a ANPD, recebe solicitações dos titulares, presta esclarecimentos, orienta colaboradores sobre práticas de proteção de dados e desempenha as demais atribuições previstas na LGPD e nas normas internas.

Nos incidentes envolvendo dados pessoais, atua de acordo com suas atribuições e com os procedimentos internos de resposta a incidentes.

9. Tratamento de dados de crianças e adolescentes

O tratamento de dados pessoais de crianças e adolescentes deve ser realizado sempre em seu melhor interesse, observadas as disposições da LGPD e as demais normas aplicáveis.

No tratamento de dados de crianças, quando utilizada a base legal do consentimento, este deverá ser específico e destacado e fornecido por pelo menos um dos pais ou pelo responsável legal, observadas as exceções previstas na legislação.

A definição da base legal adequada deve considerar a finalidade e o contexto de cada tratamento. Em caso de dúvida, consulte o Encarregado de Dados (DPO).

10. Direitos dos titulares e o ciclo de vida dos dados

SEUS DIREITOS

Entre outros direitos previstos na LGPD, o titular pode solicitar confirmação da existência de tratamento, acesso aos dados, correção de dados incompletos ou desatualizados, informações sobre compartilhamento, portabilidade, quando aplicável, eliminação dos dados tratados com consentimento nas hipóteses legais e revogação do consentimento.

CICLO DE VIDA DO DADO E O PAPEL DA FINALIDADE

Assim como tudo na vida, um dado pessoal tem um ciclo. Ele é coletado para um objetivo, ou seja, uma finalidade informada ao titular (nascimento), usado para cumprir esse objetivo (vida) e, quando a finalidade se esgota, ou seja, quando o dado deixa de ser necessário deve ser eliminado ou anonimizado de forma segura (morte/finalização do tratamento), salvo hipóteses legais que autorizem sua guarda, como cumprimento de obrigação legal ou exercício regular de direitos.

11. Boas práticas no uso de documentos

POLÍTICA DE MESA E TELA LIMPAS

- Não deixe documentos com dados pessoais expostos sobre a mesa ao se ausentar;
- Guarde documentos físicos sensíveis em armários ou gavetas trancadas ao final do expediente;
- Retire impressões da impressora imediatamente, evitando que fiquem expostas na bandeja;
- Bloqueie a tela do computador sempre que se afastar da mesa (Windows + L).

DESCARTE SEGURO

- Documentos físicos contendo dados pessoais ou informações confidenciais devem ser descartados por meio de procedimento seguro que impossibilite sua recuperação ou reidentificação, conforme as normas internas aplicáveis. Nunca descarte esses documentos diretamente no lixo comum ou na reciclagem sem a devida descaracterização.
- Mídias digitais (pen drives, HDs) fora de uso devem passar por descarte seguro conforme orientação da Gerência de TI.
- Não guarde dados por mais tempo do que o necessário; elimine-os quando o ciclo de vida do tratamento terminar.

12. Boas práticas no dia a dia

TRATAMENTO ADEQUADO

- Use dados pessoais só quando for mesmo necessário;
- Seja transparente: sempre explique por que está pedindo um dado e para que ele servirá;
- Não compartilhe dados pessoais ou informações com pessoas que não estejam autorizadas a acessá-los;

COMUNICAÇÃO E E-MAILS

O e-mail corporativo é um recurso concedido pela FINDES e deve ser usado de forma adequada. É estritamente proibido:

- Enviar dados pessoais, informações confidenciais ou restritas para ambientes externos sem autorização prévia do gestor;
- Utilizar indevidamente o nome da FINDES ou emitir opiniões pessoais que possam prejudicar a instituição ou violar direitos de terceiros;
- Enviar, armazenar ou disseminar material sexualmente explícito, ofensivo, ilegal ou contrário à legislação vigente.

Recomendações adicionais:

- Ao enviar uma mesma mensagem para diversos destinatários externos que não precisam conhecer os endereços eletrônicos uns dos outros, utilize o campo Cco (cópia oculta).
- Prefira os repositórios corporativos oficiais (ex.: SharePoint/OneDrive institucional) para armazenar documentos, evitando caixas de e-mail pessoal ou o próprio equipamento como repositório;

Desconfie de e-mails, links, anexos ou QR Codes de origem duvidosa. Na dúvida, não clique e não aponte a câmera.

USO DA INTERNET E REDE WI-FI

- Use a internet corporativa com bom senso e de acordo com nossas políticas internas;
- Nunca baixe programas de sites com alertas de segurança, nem acesse sites maliciosos (pornografia, jogos, relacionamentos);
- A rede wi-fi corporativa deve ser usada para fins institucionais, em celulares, computadores ou outros equipamentos conectados.

A FINDES pode realizar monitoramento do ambiente corporativo e dos acessos a sites, com a finalidade de garantir a segurança dos recursos tecnológicos e identificar riscos. Esse monitoramento deve estar previsto na Política de Segurança da Informação e ser comunicado de forma transparente aos colaboradores.

13. Utilização de aplicativos, sistemas e equipamentos

- O acesso aos sistemas deve seguir o princípio do privilégio mínimo cada colaborador acessa apenas as informações necessárias à sua função;
- Equipamentos de terceiros que acessem a rede corporativa devem estar adequados aos padrões de segurança da instituição;
- É proibido utilizar celular pessoal sem autorização para fotografar, receber ou compartilhar documentos, fotos ou filmagens de alunos, colaboradores dos programas do Sistema FINDES especialmente quando envolverem dados pessoais sensíveis ou imagens de crianças e adolescentes.

14. Uso de dados pessoais em inteligência artificial

Ferramentas de IA generativa vêm sendo cada vez mais utilizadas no dia a dia de trabalho. Ao utilizá-las, alguns cuidados são indispensáveis para a proteção de dados pessoais:

- Não insira dados pessoais ou sensíveis (de colaboradores, alunos, clientes ou terceiros) em ferramentas de IA que não tenham sido homologadas pela FINDES;
- Utilize somente ferramentas de IA autorizadas ou homologadas pela FINDES, observando as regras estabelecidas na Política de Uso de Inteligência Artificial.
- Verifique se há finalidade legítima e base legal antes de tratar dados pessoais com apoio de IA;
- Resultados gerados por IA devem ser revisados por um humano antes de decisões que afetem titulares de dados;
- Em caso de dúvida sobre o uso de IA com dados pessoais, consulte a política de Uso de Inteligência Artificial (POL-FINDES-017) e/ou o Encarregado de Dados (DPO);

15. Procedimentos em casos de incidentes e consequências

O QUE É UM INCIDENTE DE SEGURANÇA?

Um incidente de segurança com dados pessoais é qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou qualquer forma de tratamento inadequada ou ilícita que possa ocasionar risco aos direitos e liberdades do titular.

O QUE FAZER DIANTE DE UM INCIDENTE OU SUSPEITA

Qualquer incidente ou suspeita de comprometimento de dados pessoais deve ser comunicado imediatamente pelos canais internos definidos pela FINDES. Não é necessário aguardar a confirmação do incidente para realizar o reporte.

O tratamento do incidente segue o disposto na Política de Segurança da Informação (POL-005) e nos procedimentos de resposta a incidentes vigentes na FINDES.

CONSEQUÊNCIAS DA UTILIZAÇÃO INDEVIDA

A utilização indevida de dados pessoais pode trazer consequências previstas na Lei e na Política-008 (Gestão de Consequências e Medidas Disciplinares) da FINDES. Por isso, não compartilhe, acesse ou faça uso indevido de dados pessoais. Em caso de dúvidas, contate sempre o Encarregado de Dados Pessoais (DPO) da FINDES.

São exemplos de condutas passíveis de medidas disciplinares:

- Utilizar os recursos de tecnologia da informação para fins não relacionados às atividades da FINDES;
- Descumprir as diretrizes desta cartilha ou das políticas internas de segurança e privacidade;
- Divulgar informações confidenciais ou de propriedade da FINDES sem autorização;
- Desativar ou violar dispositivos de segurança instalados nos equipamentos;
- Não bloquear o computador ou deixar documentos/arquivos confidenciais expostos ao se ausentar;
- Compartilhar com terceiros senhas ou usuários de acesso aos recursos tecnológicos;

16. Participação em treinamentos

É imprescindível que todos os colaboradores da FINDES participem regularmente dos treinamentos oferecidos sobre LGPD, segurança da informação e temas correlatos.

Esses treinamentos visam conscientizar sobre a importância da proteção de dados pessoais, as práticas seguras no uso dos recursos tecnológicos e o cumprimento das normas internas e legais fortalecendo a cultura de segurança em toda a organização.

17. Canais de comunicação e suporte

ENCARREGADO DE DADOS (DPO)

É o ponto de contato principal para assuntos de privacidade. Em caso de dúvidas sobre o tratamento de dados ou as práticas aqui descritas, entre em contato pelo e-mail lgpd@findes.org.br.

18. Glossário

CONSENTIMENTO

Autorização clara que o titular (dono do dado) dá para que seus dados sejam usados para um fim específico.

TRATAMENTO

Qualquer ação realizada com um dado pessoal: coletar, guardar, usar, compartilhar ou excluir.

FINALIDADE

O propósito específico e informado para o qual um dado pessoal é coletado e utilizado.

NECESSIDADE

Princípio segundo o qual apenas os dados estritamente necessários à finalidade devem ser coletados.

ENCARREGADO DE DADOS (DPO)

Pessoa indicada pelo controlador para atuar como canal de comunicação entre a organização, os titulares de dados e a ANPD.

19. Referências e Recursos Adicionais

Lei Geral de Proteção de Dados (Lei nº 13.709/2018): http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Autoridade Nacional de Proteção de Dados (ANPD): https://www.gov.br/anpd/pt-br

Política de Segurança da Informação (POL-005),

Política-008 (Gestão de Consequências) e Norma de Uso dos Recursos de Tecnologia da Informação e Comunicação (NOR-025), disponíveis nos canais internos.

Política de Uso de Inteligência Artificial (POL-FINDES-017):

Política de Privacidade (POL-FINDES-014)


FINDES
SESI | SENAI | IEL | CINDES