Hernany Silveira Rocha
Lívia de Oliveira Vitola
Marcos Vinícius Beton Amorim

Cartilha sobre aplicação da

Lei Geral de Proteção de Dados Pessoais

(LGPD) na Codevasf

Brasília, DF
2026

Cartilha sobre aplicação da

Lei Geral de Proteção de Dados Pessoais

(LGPD) na Codevasf

Presidente da República Federativa do Brasil
Luiz Inácio Lula da Silva

Ministro de Estado da Integração e do Desenvolvimento Regional
Antonio Waldez Góes da Silva

Diretor Presidente da Codevasf
Lucas Felipe Oliveira

Diretor da Área de Revitalização e Desenvolvimento Territorial
José Vivaldo Souza de Mendonça Filho

Diretora da Área de Irrigação e Operações
Alessandra Cristina Rossin

Diretor da Área de Desenvolvimento e Infraestrutura
Henrique de Assis Coutinho Bernardes

Diretor da Área de Governança e Sustentabilidade
Gilliano Fred Nascimento Cutrim

Gerente-Executivo da Área de estratégia e Finanças
Milton Jesus Barbosa Junior

Gerente-Executivo da Área de Administração e Tecnologia
Gerson Vinicius Cestari Souza

Hernany Silveira Rocha
Lívia de Oliveira Vitola
Marcos Vinícius Beton Amorim

Cartilha sobre aplicação da

Lei Geral de Proteção de Dados Pessoais

(LGPD) na Codevasf

Codevasf
Brasília, DF
2026

Disponível em: https://www.codevasf.gov.br/acesso-a-informacao/institucional/biblioteca-geraldo-rocha/publicacoes

Disponível também em https://www.codevasf.gov.br/acesso-a-informacao/institucional/biblioteca-geraldo-rocha -> Catálogo on-line Sophia Biblioteca

Capa e Ilustração
Frederico Celente Lorca

Normalização Bibliográfica
Nilva Chaves
Edna Sousa Santos

Dados Internacionais de Catalogação na Publicação (CIP)

Rocha, Hernany Silveira
Cartilha sobre aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) na Codevasf / Hernany Silveira Rocha, Lívia de Oliveira Vitola, Marcos Vinícius Beton Amorim. – Brasília, DF : Codevasf, 2026.
32 p. : il.

ISBN 978-65-88380-22-2

1. Proteção de dados. 2.Segurança da informação. 3. LGPD. I. Vitola, Lívia de Oliveira. II. Amorim, Marcos Vinícius Beton. III. Título. IV. Codevasf.

CDU 342.7

Companhia de Desenvolvimento dos Vales do São Francisco e do Parnaíba – Codevasf
SGAN 601 – Conjunto I – Edifício Deputado Manoel Novaes
CEP 70830-019 Brasília - DF

SUMÁRIO

SOBRE A CARTILHA

Ao ler essa cartilha, você estará ajudando a Codevasf a implantar uma cultura de proteção de dados e adoção de procedimentos que preservam a integridade e a confidencialidade das informações pessoais sob a guarda dessa estatal.

Aqui você encontra orientações sobre princípios, práticas e responsabilidades relacionados à proteção de dados pessoais no âmbito da nossa empresa. Tudo em conformidade com a Lei nº 13.709/2018[1] – Lei Geral de Proteção de Dados Pessoais (LGPD).

O QUE É A LGPD?

A LGPD é uma legislação federal. Ela regula o tratamento de dados pessoais, com o objetivo de proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural. A LPGPD vale inclusive para os meios digitais e para os dados tratados por pessoa natural ou jurídica, de direito público ou privado.

1 BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 30 abr. 2025.

CONCEITOS FUNDAMENTAIS

Dado Pessoal: qualquer informação que identifique ou possibilite identificar uma pessoa natural, direta ou indiretamente.

Exemplos incluem dados de contato (nome, telefone, e-mail), documentos oficiais (CPF, RG, passaporte), endereços físicos e digitais (IP, geolocalização), registros de imagem ou voz, histórico de navegação e qualquer outro dado que, isolado ou combinado, permita reconhecer um indivíduo.

Dado Pessoal Sensível: dados que revelam aspectos íntimos e potencialmente discriminatórios do titular, tais como origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organizações de caráter religioso, filosófico ou político, informações referentes à saúde física ou mental, vida sexual ou orientação sexual, bem como dados genéticos ou biométricos vinculados a uma pessoa natural.

Esses dados requerem proteção redobrada, pois o uso indevido pode resultar em discriminação, estigmatização ou outras violações de direitos fundamentais. Eles estão sujeitos a medidas protetivas específicas para reduzir riscos e garantir a segurança dessas informações

Tratamento de Dados: conjunto de operações realizadas sobre dados pessoais em todo o seu ciclo de vida — da coleta à eliminação. Compreende produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, avaliação, controle, modificação, comunicação, transferência, difusão, análise, anonimização, bloqueio e descarte.

O tratamento de dados pode ser manual ou automatizado e ocorre sempre que o dado é consultado ou transformado. Cada etapa deve ter base legal, ser registrada no inventário de tratamento (ROPA) e observar os princípios da LGPD, garantindo segurança, rastreabilidade e respeito aos direitos do titular.

Anonimização/Pseudoanonimização: processos técnicos que removem ou substituem identificadores de modo que o titular não possa ser identificado, direta ou indiretamente, sem o uso de informações adicionais.

A anonimização altera permanentemente o dado (por exemplo, agregando idades em faixas), tornando-o fora do escopo da LGPD; já a pseudonimização troca identificadores por códigos ou pseudônimos mantidos em arquivo separado e protegido, possibilitando reidentificação controlada quando estritamente necessária.

Essas técnicas reduzem riscos de vazamento, facilitam o compartilhamento para pesquisa e estatísticas e devem ser aplicadas seguindo padrões reconhecidos, como ISO/IEC 20889, garantindo a irreversibilidade (no caso da anonimização) ou o controle rigoroso da chave de reidentificação (no caso da pseudonimização)

QUEM SÃO OS ATORES DA LGPD

Controlador de dados: pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais. É responsável por definir a finalidade, a base legal, os meios de processamento, bem como por garantir a conformidade com a LGPD, responder às solicitações dos titulares, adotar medidas de segurança e demonstrar prestação de contas perante a ANPD.

Na Codevasf o Controlador de Dados é o Diretor-Presidente da empresa.

Encarregado de Dados (Data Protection Officer - DPO): pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares e a ANPD. Suas atribuições incluem orientar colaboradores sobre práticas de proteção de dados, receber e encaminhar reclamações dos titulares, cooperar com a autoridade de supervisão, monitorar a conformidade interna, elaborar relatórios de impacto e recomendar melhorias de segurança e governança. O DPO deve possuir conhecimento jurídico-regulatório e técnico em privacidade, ter autonomia funcional e estar acessível publicamente por meio de contato oficial.

Na Codevasf, o Encarregado de Dados é nomeado pelo Diretor-Presidente da empresa para desempenhar essas funções.

Titular de Dados: pessoa natural a quem se referem os dados e que, por isso, possui direitos assegurados pela LGPD, tais como confirmação de existência, acesso, correção, anonimização, bloqueio, eliminação, portabilidade, informação sobre compartilhamento e revogação do consentimento. O titular pode exercer esses direitos a qualquer momento, por meio de solicitação gratuita aos agentes de tratamento, devendo receber resposta clara e tempestiva.

O tratamento de dados pode ser manual ou automatizado e ocorre sempre que o dado é consultado ou transformado. Cada etapa deve ter base legal, ser registrada no inventário de tratamento (ROPA) e observar os princípios da LGPD, garantindo segurança, rastreabilidade e respeito aos direitos do titular.

Operador de Dados: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador e estritamente de acordo com suas instruções. O operador deve aplicar salvaguardas de segurança equivalentes às do controlador, manter registros detalhados das atividades de processamento, cooperar para o atendimento aos direitos dos titulares, comunicar imediatamente incidentes de segurança e envolver suboperadores apenas com autorização expressa, garantindo cláusulas contratuais de proteção de dados.

Na Codevasf foram nomeados gestores de dados, por meio da Decisão 961/2024 para realizarem essas atribuições e colaborar na implantação da LGPD.

PRINCÍPIOS DA LGPD: PROTEGENDO SEUS DADOS PESSOAIS

A Lei Geral de Proteção de Dados Pessoais (LGPD) estabelece um conjunto de princípios que servem como bússola para as atividades de tratamento de dados no Brasil. Esses princípios formam a base ética e jurídica que orienta empresas e órgãos públicos a coletar, usar, armazenar e compartilhar informações pessoais de maneira responsável.

Quando você compreende e aplica os princípios da LGPD , você garante a conformidade legal. O mais importante é que você ajuda a empresa a construir a confiança junto aos titulares dos dados. Essa forma de agir deixa claro que o tratamento das informações respeita os direitos fundamentais e promove a cultura de privacidade.

- **Finalidade:** O tratamento de dados deve ter um propósito legítimo, específico e informado ao titular.
- **Necessidade:** Devem ser coletados apenas os dados estritamente essenciais para a finalidade declarada.
- **Adequação:** O uso dos dados deve ser compatível com a finalidade informada e o contexto da coleta.
- **Segurança:** Medidas técnicas e administrativas devem proteger os dados contra acessos não autorizados, perdas e violações.
- **Prevenção:** É necessário adotar práticas para evitar incidentes que possam comprometer a privacidade dos dados.
- **Transparência:** Os titulares têm direito a informações claras sobre o tratamento de seus dados.
- **Livre Acesso:** o direito de consultar e obter informações sobre seus dados deve ser garantido aos titulares.
- **Qualidade dos Dados:** As informações devem ser exatas, completas, atualizadas e pertinentes ao seu uso.

- **Não Discriminação:** Os dados não podem ser utilizados para discriminar ou prejudicar os titulares.
- **Responsabilização e Prestação de Contas:** Controladores e operadores devem demonstrar que seguem práticas adequadas de proteção de dados.

Isso quer dizer que as empresas e órgãos públicos que tratam dados de pessoa devem sempre:

- deixar claro por que estão coletando as informações;
- limitar essa coleta ao mínimo necessário;
- usar os dados apenas para o que foi combinado;
- garantir a segurança dos dados;
- permitir que o titular saiba e controle como seus dados são utilizados;
- manter as informações atualizadas e corretas;
- assegurar que os dados coletados não sejam usados para discriminar o titular;
- demonstrar que cumprem todas essas obrigações.

PASSOS PRÁTICOS PARA A PROTEÇÃO DE DADOS

Nesta seção, você encontrará dicas simples e diretas para aplicar a Lei Geral de Proteção de Dados (LGPD) no seu dia a dia na Codevasf. São práticas que ajudam a transformar os princípios da lei em ações concretas, reduzindo riscos e fortalecendo a confiança.

Siga estas orientações para garantir a segurança e a privacidade das informações que você manuseia.

1 Identificação e Classificação dos Dados

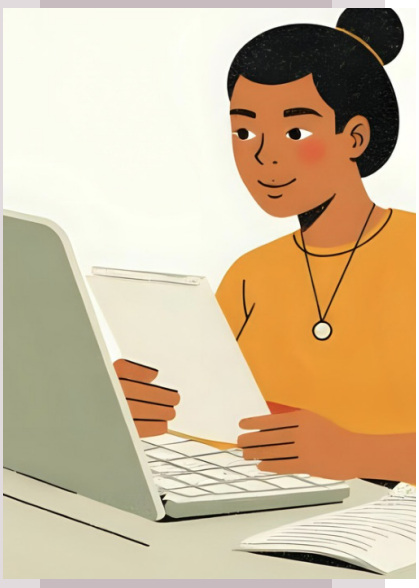
- Identifique os Dados: Mapeie os dados pessoais que você coleta, como nome, e-mail, CPF, telefone e endereço.
- Verifique Dados Sensíveis: Identifique se há dados sensíveis, como saúde, crenças religiosas, orientação sexual ou biometria.
- Classifique os Dados: Separe os dados entre "Pessoais" e "Sensíveis", definindo o nível de proteção necessário.
- Documente: Mantenha um inventário atualizado, especificando quem tem acesso e para que são usados.

2 Verificação da Aplicabilidade da LGPD

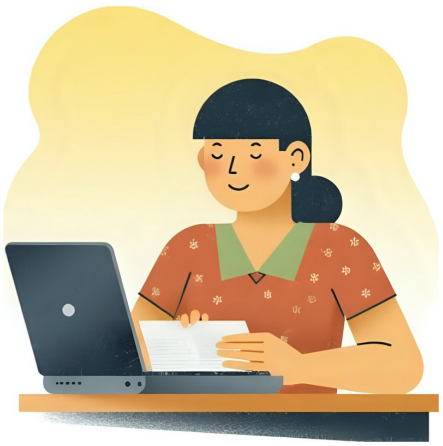
- Pergunte-se: estou lidando com dados que podem identificar uma pessoa?
- Lembre-se: a LGPD se aplica mesmo que o tratamento não seja comercial.
- Avalie se os dados são tratados no Brasil ou pertencem a pessoas localizadas no país.

3 Definição da Base Legal e Finalidade

- Defina o motivo pelo qual você está tratando os dados:
    1. Cumprimento de obrigação legal?
    2. Execução de políticas públicas?
    3. Realização de pesquisas?
- Garanta que a finalidade do uso dos dados seja clara e documentada.
- Informe o titular sobre como seus dados serão usados, garantindo transparência.



4 Controle de Acesso e Compartilhamento



- Restrinja o Acesso: Permita que apenas pessoas autorizadas acessem os dados.
- Use Canais Seguros: Prefira e-mail corporativo ou sistemas internos para compartilhar informações.
- Registre o Compartilhamento: Documente a finalidade e os destinatários dos dados.
- Não Compartilhe Sem Necessidade: Antes de enviar informações, pergunte-se: o destinatário realmente precisa desses dados?
- Certifique-se de que há Base Legal: Para qualquer compartilhamento, confirme que existe uma justificativa legal.

5 Proteção de Dados Sensíveis

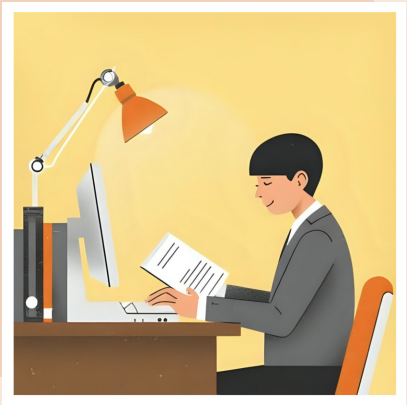
- Evite divulgar dados sensíveis (saúde, religião, orientação sexual) em documentos públicos.
- Sempre que possível, anonimize ou generalize os dados (exibir apenas iniciais, faixas etárias).
- Em documentos públicos, publique apenas versões resumidas e convertidas em formato não editável (PDF).
- Remova metadados dos arquivos antes de compartilhá-los.
- Registre internamente a justificativa para qualquer divulgação de dado sensível.

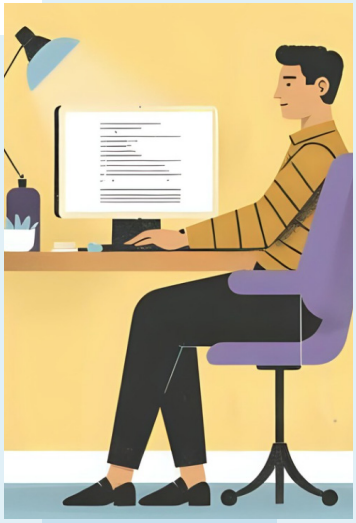
6 Segurança e Sigilo

- Use Canais Oficiais: Priorize o e-mail corporativo ou sistemas internos para tratar questões de dados pessoais.
- Evite Aplicativos de Mensagens Pessoais: Não use WhatsApp ou outras plataformas pessoais para compartilhar dados.
- Controle de Acesso: Identifique o assunto e a finalidade ao enviar documentos que contenham dados pessoais.
- Autenticação: Mantenha o controle de acesso com senhas seguras e autenticação em dois fatores, quando aplicável.
- Registre os Acessos: Documente quem visualizou documentos sensíveis, mantendo um histórico de acesso.
- Treinamento: Participe de treinamentos e mantenha-se atualizado sobre boas práticas de proteção de dados

7 Anonimização e Pseudonimização

- Anonimize os Dados: Sempre que possível, transforme dados pessoais em informações não identificáveis.
- Pseudonimização: Substitua identificadores diretos por códigos, garantindo que a reidentificação só ocorra com controle rigoroso.
- Utilize essas técnicas em pesquisas, análises e sempre que precisar compartilhar dados de forma segura.





8 Manutenção e Descarte Seguro

- Armazene os Dados de Forma Segura: Utilize sistemas corporativos protegidos.
- Descarte Dados Obsoletos: Elimine dados que não sejam mais necessários, seguindo uma política de descarte segura.
- Faça Backups Seguros: Garanta que os dados essenciais sejam armazenados com segurança e possam ser recuperados em caso de incidente.

9 Monitoramento e Auditoria

- Realize auditorias periódicas para garantir a conformidade com a LGPD.
- Mantenha registros de tratamento de dados (inventário), documentando a base legal, finalidade e prazo de retenção.
- Monitore o acesso aos sistemas que contêm dados pessoais, garantindo rastreabilidade.

10 Atendimento ao Titular dos Dados

- Facilite o acesso dos titulares aos seus dados pessoais. Garanta que possam solicitar a correção, atualização ou exclusão de seus dados.
- Ofereça um canal claro e acessível para que os titulares tirem dúvidas ou exerçam seus direitos.
- Em caso de dúvida, acione o Subcomitê de Proteção de Dados ou a área de TI.

CUIDADOS ESSENCIAIS EM RELAÇÃO À LGPD NA CODEVASF

As condutas a seguir, devem ser adotadas na Codevasf para garantir a conformidade com a LGPD, com exemplos práticos que ilustram o que é considerado adequado no tratamento de dados pessoais:

1 Coleta e Armazenamento de Dados Pessoais

Situação	Conduta adequada	Exemplo prático na Codevasf
Coleta de Dados de Beneficiários	Garantir que os dados coletados sejam apenas os necessários para o programa ou projeto.	Ao cadastrar beneficiários de obras de saneamento, solicitar apenas nome, CPF e endereço, evitando coletar dados sensíveis desnecessários.
Armazenamento de Dados Pessoais	Utilizar sistemas seguros, com acesso restrito e protegido por senhas.	Os dados dos beneficiários são armazenados em sistema interno com acesso limitado apenas a funcionários autorizados.
Compartilhamento de Dados	Garantir que o compartilhamento seja realizado apenas com parceiros autorizados e com base legal.	Compartilhar dados de beneficiários com empresas contratadas para execução de obras apenas mediante contrato com cláusulas de proteção de dados.

2 Tratamento de Dados de Servidores e Colaboradores

Situação	Conduta adequada	Exemplo prático na Codevasf
Dados de Folha de Pagamento	Tratar dados pessoais dos servidores para cumprimento de obrigação legal, como pagamento de salários e impostos.	O setor de Recursos Humanos coleta dados bancários e CPF dos servidores para processamento da folha de pagamento.
Controle de Frequência	Garantir que o controle de ponto seja realizado de forma segura, com dados armazenados em sistema protegido.	O sistema de ponto eletrônico da Codevasf é protegido por senha e acesso controlado.
Dados de Saúde	Tratar dados de saúde de servidores apenas quando necessário para fins de licença médica ou saúde ocupacional.	O RH solicita atestado médico para afastamento do servidor por motivos de saúde e mantém os documentos em sigilo.

3 Comunicação e Marketing

Situação	Conduta adequada	Exemplo prático na Codevasf
Envio de E-mails Promocionais	Enviar e-mails apenas para destinatários que tenham dado consentimento ou que sejam parte de um relacionamento institucional.	Enviar informações sobre programas de desenvolvimento regional apenas para inscritos que solicitaram o recebimento.
Publicação de Imagens	Obter o consentimento dos participantes antes de publicar imagens em eventos institucionais.	Antes de divulgar fotos de um evento, os participantes são informados e autorizam o uso de sua imagem.
Uso de Redes Sociais	Garantir que as imagens e informações publicadas não exponham dados pessoais sem autorização.	Publicar imagens de projetos concluídos, sem divulgar informações pessoais dos beneficiários.

4 Segurança da Informação

Situação	Conduta adequada	Exemplo prático na Codevasf
Controle de Acesso	Garantir que apenas funcionários autorizados possam acessar sistemas que contenham dados pessoais.	O sistema de cadastro de beneficiários tem acesso restrito apenas aos funcionários do setor responsável.
Proteção Contra Vazamento	Implementar medidas de segurança como criptografia e autenticação em dois fatores.	O acesso ao sistema de gestão de documentos é feito por meio de login e senha, com autenticação em duas etapas.
Treinamento de Colaboradores	Realizar treinamentos periódicos sobre a LGPD e boas práticas de segurança da informação.	Todos os funcionários recebem treinamento anual sobre proteção de dados pessoais.

5 Atendimento ao Titular dos Dados

Situação	Conduta adequada	Exemplo prático na Codevasf
Solicitação de Acesso aos Dados	Facilitar o acesso dos titulares aos seus dados pessoais, garantindo resposta em prazo razoável.	Um beneficiário solicita informações sobre seus dados cadastrados, e a Codevasf fornece as informações em até 15 dias.
Solicitação de Correção de Dados	Permitir que os titulares solicitem a correção de dados incorretos ou desatualizados.	Um colaborador solicita a correção de seu endereço residencial no sistema de RH.
Solicitação de Exclusão de Dados	Excluir os dados pessoais dos titulares quando solicitado, exceto se houver obrigação legal para mantê-los.	Um beneficiário solicita a exclusão de seu cadastro após o término do programa, e a Codevasf remove os dados.

6 Transparência e Comunicação

Situação	Conduta adequada	Exemplo prático na Codevasf
Política de Privacidade	Disponibilizar uma política de privacidade clara e acessível para os cidadãos.	A Codevasf publica em seu site uma política de privacidade que explica como os dados dos beneficiários são tratados.
Notificação de Incidentes	Informar aos titulares e à ANPD – Autoridade Nacional de Proteção de Dados, órgão do governo federal responsável por fiscalizar e garantir o cumprimento da LGPD, em caso de incidente de segurança que envolva dados pessoais.	Em caso de vazamento de dados de beneficiários, a Codevasf notifica imediatamente a ANPD e os titulares afetados.
Consentimento	Obter o consentimento dos titulares para o tratamento de seus dados, quando necessário.	Ao participar de um programa de capacitação, o participante assina um termo de consentimento para uso de sua imagem e dados.

7 Monitoramento e Auditoria

Situação	Conduta adequada	Exemplo prático na Codevasf
Avaliação de Conformidade	Realizar auditorias periódicas para verificar o cumprimento da LGPD.	O setor de auditoria interna da Codevasf realiza uma verificação semestral da conformidade com a LGPD.
Monitoramento de Acesso	Registrar e monitorar o acesso aos sistemas que contêm dados pessoais.	O sistema de cadastro de beneficiários registra o login e logout de todos os usuários.
Acompanhamento de Reclamações	Manter um canal de comunicação para receber e responder a reclamações de titulares de dados.	A Ouvidoria da Codevasf recebe e acompanha reclamações relacionadas ao tratamento de dados pessoais.

EXEMPLOS DE **CONDUTA INADEQUADA** EM RELAÇÃO À LGPD

Os exemplos a seguir ilustram como falhas de governança e descuidos operacionais podem expor a Codevasf a sanções legais, danos na reputação e perda de confiança.
Reconhecer tais comportamentos ajuda a promover uma cultura de conformidade e respeito à privacidade, tanto em rotinas mais simples como em processos complexos.

- Enviar planilhas com dados pessoais de clientes ou empregados por e mail sem criptografia ou senha de proteção;
- Compartilhar listas contendo CPF, endereço e salário em grupos de mensagens instantâneas (WhatsApp, Telegram) não oficiais;
- Publicar relatórios em intranet ou internet com informações de saúde ou filiação sindical sem anonimização;
- Coletar cópias de documentos (RG, CNH) quando não há base legal ou finalidade clara para tal exigência;
- Armazenar dados pessoais em pen drives ou HDs externos sem controle de acesso ou backup;
- Manter banco de dados com usuários genéricos (ex.: "admin/admin") ou sem autenticação multifator;
- Utilizar dados para fins diferentes do propósito original, como repassar contatos de fornecedores a empresas de marketing;
- Ignorar solicitações de titulares que pedem correção ou exclusão de seus dados.
- Conceder acesso irrestrito a estagiários ou terceiros a sistemas que armazenam informações sensíveis;
- Não registrar incidentes de segurança ou atrasar a comunicação de vazamentos aos titulares e à ANPD - Autoridade Nacional de Proteção de Dados, órgão do governo federal responsável por fiscalizar e garantir o cumprimento da LGPD,

BOAS PRÁTICAS INDISPENSÁVEIS PARA PROTEGER DADOS PESSOAIS

Mantenha a privacidade e segurança dos dados pessoais seguindo estas orientações essenciais:

Mantenha o Sigilo e Controle de Acesso

- Use a ferramenta oficial (E-Codevasf/Protocolo) e marque documentos como "restritos" sempre que necessário;
- Em contratos ou convênios, inclua cláusulas de confidencialidade, garantindo o dever de sigilo;
- Registre o tratamento de dados: documente a base legal, a finalidade, os responsáveis e o prazo de retenção;
- Mantenha um log de acessos, registrando quem visualizou documentos sensíveis.

Proteja os Dados de Saúde e Informações Sensíveis

- Divulgue informações de saúde ou outros dados sensíveis apenas quando houver base legal, ordem judicial ou necessidade processual clara;
- Sempre que possível, anonimize ou generalize os dados antes de divulgá-los;
- Em documentos públicos, oculte ou generalize dados sensíveis, garantindo que apenas informações essenciais sejam visíveis.

DÚVIDAS FREQUENTES

1 Perguntas Comuns sobre a LGPD

Pergunta	Resposta	Exemplo prático na Codevasf
Quais são as principais bases legais para tratamento?	As bases legais são: consentimento, cumprimento de obrigação legal, execução de políticas públicas, proteção da vida, tutela da saúde, legítimo interesse, entre outras.	Tratamento de dados de saúde para controle de licença médica é uma obrigação legal para o empregador.
É necessário consentimento para tratar dados pessoais?	O consentimento é a regra geral para o tratamento de dados. Entretanto, a LGPD estabelece nove exceções que dispensam o consentimento.	A coleta de dados para folha de pagamento não exige consentimento, pois é uma obrigação legal.
O que é o consentimento do titular?	É a autorização dada pelo titular de forma livre, informada e inequívoca, permitindo o tratamento de seus dados.	Ao se cadastrar em um serviço online, o usuário concede consentimento ao aceitar os termos de uso.
Quando o consentimento não é necessário?	Quando o tratamento for baseado em outras bases legais, como cumprimento de obrigação legal ou interesse legítimo.	A coleta de dados de funcionários para cumprimento de obrigações trabalhistas não exige consentimento.
O que são dados pessoais sensíveis?	São dados que revelam origem racial, opinião política, religião, saúde, vida sexual, dados genéticos ou biométricos.	Dados de saúde de funcionários coletados para controle de afastamentos são considerados sensíveis.

Pergunta	Resposta	Exemplo prático na Codevasf
O que é tratamento de dados pessoais?	É qualquer operação realizada com os dados, como coleta, armazenamento, uso, compartilhamento ou eliminação.	O cadastro de clientes em um sistema de vendas é uma forma de tratamento de dados pessoais.
Quem são os agentes de tratamento?	O controlador (quem decide sobre o tratamento dos dados) e o operador (quem realiza o tratamento em nome do controlador).	Uma empresa que terceiriza o processamento da folha de pagamento tem o operador como a empresa terceirizada.
O que é um incidente de segurança de dados?	É qualquer evento que comprometa a segurança dos dados pessoais, como vazamento, perda ou acesso não autorizado.	Um ataque hacker que expõe informações de clientes é um incidente de segurança.
Como posso exercer meus direitos como titular de dados?	Você pode solicitar diretamente ao controlador (empresa, órgão público) o acesso, correção ou exclusão de seus dados.	Enviar um e-mail ao RH solicitando a atualização de seu endereço cadastrado.
O que é a portabilidade de dados?	É o direito do titular de solicitar que seus dados sejam transferidos para outro fornecedor de serviço.	Um cliente pode solicitar que seus dados sejam transferidos de um banco para outro.

2 Perguntas sobre Direitos dos Titulares dos Dados

Pergunta	Resposta	Exemplo prático na Codevasf
Como posso solicitar acesso aos meus dados?	Você deve entrar em contato via sistema FalaBR, abrir um pedido de solicitação a respeito das informações tratadas sobre você.	Solicitar informações a respeito da sua folha de pagamento.
Posso pedir para corrigir informações incorretas?	Sim. Você tem o direito de solicitar via sistema FalBR a correção de dados incompletos, inexatos ou desatualizados.	Solicitar a correção do seu endereço no cadastro do empregado.
Posso pedir para excluir meus dados?	Sim, você pode solicitar a exclusão, via sistema FalaBR exceto se houver uma obrigação legal para mantê-los.	Solicitar a exclusão de informações referentes a multas prescritas de tarifa de água (K1).
O que é o direito de revogar o consentimento?	É o direito de retirar o consentimento previamente dado para o tratamento de seus dados pessoais.	Cancelar o consentimento para receber e-mails.
O que é o direito de anonimização?	É o direito de transformar os dados pessoais em informações que não possam ser relacionadas a uma pessoa específica.	Solicitar que um sistema transforme seu nome em um código para proteger sua identidade.
Como posso saber com quem meus dados foram compartilhados?	Você tem o direito de solicitar via sistema FalaBR ao controlador uma lista das entidades com as quais seus dados foram compartilhados.	Pedir que informe com quais entidades seus dados foram compartilhados.
O que é o direito de portabilidade?	É o direito de solicitar que seus dados sejam transferidos para outro fornecedor de serviço ou produto.	Solicitar que seus dados sejam transferidos no caso de migração de plano de previdência privada.

3 Perguntas sobre Medidas de Segurança

Pergunta	Resposta	Exemplo prático na Codevasf
Quais são as principais medidas de segurança de dados?	Controle de acesso, criptografia, backup, políticas de segurança e treinamento de colaboradores.	Utilizar senha forte e autenticação em dois fatores para acessar sistemas corporativos.
Como proteger os dados em trânsito?	Utilizando criptografia para garantir que os dados sejam transmitidos de forma segura.	Enviar e-mails com informações sensíveis utilizando criptografia de ponta a ponta.
O que é um Plano de Resposta a Incidentes?	É um conjunto de procedimentos para identificar, conter, mitigar e comunicar incidentes de segurança de dados.	Ter uma equipe de segurança preparada para responder rapidamente a um vazamento de dados.
Quando devo notificar um incidente de segurança?	Sempre que houver risco para os titulares dos dados, a notificação deve ser feita à ANPD e aos titulares afetados.	Notificar os clientes afetados em caso de vazamento de informações bancárias.
Quem é responsável pela segurança dos dados?	Todos os colaboradores têm responsabilidade, mas o controlador e o operador devem garantir a implementação de medidas de segurança.	O setor de TI deve garantir a proteção dos sistemas e o setor de RH deve proteger os dados de funcionários.
O que é anonimização de dados?	É o processo de tornar os dados pessoais irreconhecíveis, de forma que não possam ser relacionados a uma pessoa.	Converter o nome de um cliente em um código numérico para fins de pesquisa.
O que é pseudonimização?	É o processo de substituir dados pessoais por identificadores artificiais, mantendo a possibilidade de reidentificação.	Utilizar códigos para substituir os nomes de pacientes em uma pesquisa médica.

4 Perguntas Frequentes para a Administração Pública

Pergunta	Resposta	Exemplo prático na Codevasf
A LGPD se aplica à Codevasf?	Sim. A LGPD é aplicável a todos os órgãos e entidades da administração pública, incluindo empresas públicas e sociedades de economia mista, como a Codevasf.	A Codevasf deve garantir a proteção dos dados pessoais de servidores, colaboradores e cidadãos atendidos em seus programas.
Quem é o controlador dos dados na Codevasf?	O Diretor-Presidente da Codevasf é o controlador dos dados pessoais, responsável pelas decisões referentes ao tratamento desses dados.	O Diretor-Presidente delega ações necessárias para operacionalizar a Política de Proteção de Dados Pessoais dentro da estrutura organizacional.
O que é o encarregado pelo tratamento de dados pessoais na Codevasf?	O encarregado de dados é a pessoa indicada pelo controlador ou operador que atua como canal de comunicação entre o controlador, os titulares dos dados e a ANPD.	Ter uma equipe de segurança preparada para responder rapidamente a um vazamento de dados.
Na Codevasf, o encarregado de dados e seu substituto são nomeados pelo Diretor-Presidente e recebe as solicitações via sistema FalaBR.	Ponto de contato para os titulares dos dados, as autoridades e a própria Codevasf.	Notificar os clientes afetados em caso de vazamento de informações bancárias.
É necessário consentimento para tratar dados pessoais na Codevasf?	O consentimento é a regra geral no que tange ao tratamento de dados pessoais, todavia, existem exceções.	Para o cumprimento de obrigações legais, como envio de informações ao eSocial, não é necessário consentimento.

Pergunta	Resposta	Exemplo prático na Codevasf
Como a Codevasf compartilha dados pessoais com outros órgãos?	O compartilhamento de dados pela administração pública é permitido para o atendimento de sua finalidade pública, na persecução do interesse público, respeitando os princípios da LGPD.	Compartilhamento de dados com o Ministério do Desenvolvimento Regional para execução conjunta de projetos.
Quais medidas de segurança a Codevasf adota para proteger os dados pessoais?	A Codevasf implementa medidas técnicas e administrativas para proteger os dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.	Utilização de sistemas de controle de acesso, criptografia de dados sensíveis e treinamentos periódicos para os colaboradores.
Como os titulares podem exercer seus direitos na Codevasf?	Os titulares podem entrar em contato via sistema FalaBR, abrir um pedido de solicitação a respeito das informações tratadas.	Envio de solicitação por meio da plataforma Fala.BR ou diretamente à encarregada, conforme informações disponíveis no site da Codevasf.
O que é o Comitê Gestor de Proteção de Dados Pessoais da Codevasf?	É o órgão responsável por analisar e revisar políticas, diretrizes e normas relacionadas à proteção de dados pessoais na Codevasf, além de assessorar o controlador e propor ações de conscientização.	O Comitê propõe a implementação de políticas de segurança da informação e promove ações de capacitação sobre a LGPD.
Onde encontrar mais informações sobre a Política de Privacidade e Proteção de Dados Pessoais da Codevasf?	As informações estão disponíveis no site oficial da Codevasf, na seção de acesso à informação.	Acesse: Política de Privacidade e Proteção de Dados Pessoais - Codevasf

CONTATOS E MAIS INFORMAÇÕES

Política de Privacidade e Proteção de Dados Pessoais – Codevasf:

https://www.codevasf.gov.br/acesso-a-informacao/institucional/legislacao/estatuto-regimentos-politicas-e-regulamentos/politicas/politica-de-privacidade-e-protecao-de-dados-pessoais.pdf

Autoridade Nacional de Proteção de Dados (ANPD):

https://www.gov.br/anpd/pt-br

Em caso de dúvida entre em contato com o Subcomitê de Proteção de Dados Pessoais da Codevasf ou consulte o Encarregado de Dados (DPO).

www.codevasf.gov.br

 instagram.com/codevasf

 facebook.com/codevasf

 linkedin.com/company/codevasf

 youtube.com/codevasfoficial

CODEVASF

MINISTÉRIO DA INTEGRAÇÃO E DO DESENVOLVIMENTO REGIONAL

GOVERNO DO BRASIL
DO LADO DO POVO BRASILEIRO

ISBN: 978-65-88380-22-2
CBL
9 786588 380222