

MÓDULO 5

Dados do Cooperado: Um Tesouro Sob Nossa Guarda



Dados do Cooperado: Um tesouro sob nossa guarda e a responsabilidade na era da LGPD

Os dados pessoais e financeiros dos cooperados são o ativo mais valioso e sensível de uma cooperativa de crédito, um verdadeiro **tesouro sob nossa guarda**. Este artigo aborda a responsabilidade legal e ética de proteger essas informações, em conformidade com a **Lei Geral de Proteção de Dados (LGPD)**. Detalhamos a **identificação de informações sensíveis** (como CPF, renda e dados de saúde), os **riscos de vazamentos acidentais** (e-mail errado, conversas em público) e a **regra de ouro** para o compartilhamento seguro e legal de dados. O objetivo é transformar a proteção de dados em uma prioridade cultural, garantindo a privacidade do cooperado e a credibilidade da cooperativa.

Palavras-chave: LGPD, Dados Pessoais Sensíveis, Vazamento de Dados, Privacidade, Cooperativismo de Crédito, Compartilhamento Seguro.

1. Introdução: A LGPD e a nova era da proteção de dados

A **Lei Geral de Proteção de Dados (LGPD)** [1] estabeleceu um novo marco legal no Brasil, conferindo aos cidadãos o controle sobre suas informações pessoais e impondo responsabilidades rigorosas às organizações que as tratam. Para cooperativas de crédito, que lidam diariamente com um volume imenso de dados financeiros e pessoais, a LGPD não é apenas uma lei a ser cumprida, mas um **compromisso de confiança** com o cooperado.

Dados do Cooperado: O Ativo mais sensível. Em uma cooperativa, o dado do cooperado é o coração do negócio. Ele inclui desde informações cadastrais básicas até detalhes sobre movimentações financeiras, histórico de crédito e, em alguns casos, informações de saúde (para seguros, por exemplo). A proteção desse "tesouro" é fundamental para a sustentabilidade e reputação da instituição.

2. Identificação de informações Sensíveis

A LGPD distingue entre **Dados Pessoais** e **Dados Pessoais Sensíveis**. Ambos exigem proteção, mas o tratamento dos sensíveis é ainda mais restrito.



Categoria de Dados	Exemplos Comuns em Cooperativas	Nível de Sensibilidade
Dados Pessoais	Nome, CPF, RG, Endereço, E-mail, Telefone, Dados de conta e agência.	Alto
Dados Pessoais Sensíveis	Origem racial ou étnica, convicções religiosas, dados de saúde (ex: laudos médicos para seguros), dados biométricos.	Muito Alto
Informações Financeiras	Renda, Histórico de crédito, Transações bancárias, Investimentos.	Crítico

Diretriz Prática: Todo colaborador deve tratar **qualquer informação** que possa identificar um cooperado como confidencial. O vazamento de um CPF ou de um extrato de conta é um incidente grave que pode levar a fraudes contra o cooperado e a multas severas para a cooperativa.

3. Os riscos de vazamentos acidentais (O Fator Humano)

A maioria dos vazamentos de dados em instituições financeiras não ocorre por ataques cibernéticos sofisticados, mas sim por **erros operacionais e descuido humano** [2].

3.1. E-mail enviado para o destinatário errado

Este é um dos incidentes mais comuns. Um colaborador anexa um extrato ou um contrato contendo dados de um cooperado e, por engano, envia para o e-mail de outro cooperado ou de um destinatário externo.

Estudo de Caso Prático: Um funcionário do setor de crédito envia uma planilha com o nome e a renda de 50 cooperados para um fornecedor, em vez de enviar a planilha de acompanhamento de projetos. O erro é percebido 3 horas depois. A cooperativa precisa notificar a **Autoridade Nacional de Proteção de Dados (ANPD)** e todos os 50 cooperados sobre o incidente, além de arcar com os custos de remediação e o risco de multa.

3.2. Conversas em locais públicos

Discutir detalhes de contas, transações ou situações financeiras de cooperados em locais públicos (restaurantes, elevadores, *home office* com outras pessoas presentes) é uma violação de privacidade. A informação pode ser facilmente capturada por escuta accidental ou intencional (*Shoulder Surfing*).

3.3. Descarte incorreto de documentos

Documentos impressos contendo dados (formulários, rascunhos, relatórios) devem ser descartados em trituradoras de papel seguras. Jogá-los no lixo comum é um convite aberto para a coleta de informações por criminosos.

4. A regra de ouro para o compartilhamento seguro de dados

O tratamento e o compartilhamento de dados devem seguir o princípio da **necessidade** e da **segurança**. Esse princípios norteiam a forma como os dados podem ou devem ser compartilhados.

4.1. Princípio da necessidade (Mínimo necessário)

O colaborador só deve acessar e compartilhar os dados **estritamente necessários** para a execução de sua função, ou seja exige que haja um cuidado extra e uma atenção especial em cada documento que é compartilhado. Se você precisa enviar um documento para um cooperado, certifique-se de que ele contenha apenas as informações pertinentes e que não exponha dados de terceiros.

4.2. A regra de ouro: Canais oficiais e criptografia



“ O compartilhamento de dados do cooperado deve ser feito exclusivamente por canais oficiais, criptografados e autorizados pela cooperativa.” ,”

Tipo de Compartilhamento	Canal Autorizado	Canal NÃO Autorizado (Risco Alto)
Interno (Colaborador para Colaborador)	Sistemas de gestão internos, E-mail corporativo criptografado.	WhatsApp pessoal, E-mail pessoal (Gmail, Outlook), Conversa em público.
Externo (Cooperativa para Cooperado)	Aplicativo oficial da cooperativa, Área logada no site, E-mail corporativo com proteção de senha/criptografia.	WhatsApp pessoal do colaborador, SMS sem criptografia.
Regulatório/Legal	Plataformas seguras da ANPD, Banco Central ou órgãos judiciais, seguindo protocolo de TI.	E-mail comum sem criptografia.

Diretriz para Implementação: Nunca utilize canais de comunicação pessoais para tratar de assuntos que envolvam dados de cooperados. Em caso de dúvida sobre a segurança de um canal, consulte a equipe de TI ou o Encarregado de Dados (DPO) da cooperativa.

5. Conclusão



A proteção dos dados do cooperado é o reflexo do compromisso da cooperativa com seus valores fundamentais. Na era da LGPD, cada colaborador é um **agente de privacidade**. Ao identificar corretamente as informações sensíveis, evitar vazamentos acidentais e aderir rigorosamente à regra de ouro do

compartilhamento seguro, a cooperativa não só cumpre a lei, mas também reforça o pilar mais importante de sua existência: a **confiança** mútua com seus cooperados.

Referências Bibliográficas

- [1] Somos Cooperativismo. **Bases Legais - LGPD**. Disponível em: <https://somoscooperativismo.coop.br/lgpd/bases-legais>
- [2] Grant Thornton. **LGPD: como proceder em casos de vazamento de dados?**. Disponível em: <https://www.grantthornton.com.br/insights/artigos-e-publicacoes/lgpu-como-proceder-em-casos-de-vazamento-de-dados/>
- [3] MundoCoop. **Por que as cooperativas financeiras precisam estar em dia com a LGPD?**. Disponível em: <https://mundocoop.com.br/destaque/por-que-as-cooperativas-financeiras-precisam-estar-em-dia-com-a-lgpd/>
- [4] (Adicionar referências adicionais conforme aprofundamento da pesquisa, se necessário).