INSTITUTO FEDERAL DE MINAS GERAIS
CAMPUS SÃO JOÃO EVANGELISTA
SISTEMAS DE INFORMAÇÃO

LUCAS GOMES FERNANDES
PATRÍCIA DA SILVA COSTA
VALDIR DE SOUZA CARVALHO NETO
VINÍCIUS GOMES FERNANDES

PROTEÇÃO DE DADOS - ATIVIDADE 01

SÃO JOÃO EVANGELISTA
2025

1. Diagnóstico do Caso

O incidente na Fintech representa uma falha crítica de segurança que resultou no vazamento de dados pessoais, como nome e CPF, e dados pessoais sensíveis, como informações de saúde. Este último tipo de dado exige proteção redobrada, pois sua exposição pode levar à discriminação. Todo o processo, desde a coleta até o armazenamento, é considerado tratamento de dados, e o vazamento configura uma atividade de tratamento ilegal que violou o direito fundamental à privacidade dos clientes.

A principal falha de segurança foi a quebra da confidencialidade, pilar que assegura o acesso à informação apenas por pessoas autorizadas. Além disso, a alegação da empresa de que os dados estavam anonimizados se mostrou ineficaz, já que a simples correlação de informações permitia a identificação dos indivíduos, demonstrando uma falha técnica grave no processo de proteção.

2. Comparativo com um Caso Real: Equifax (2017)

Este cenário é muito similar ao vazamento da Equifax, uma das maiores agências de crédito dos EUA. Em 2017, a empresa admitiu que hackers exploraram uma vulnerabilidade conhecida em seu sistema, que não havia sido corrigida a tempo, expondo dados de 147 milhões de pessoas. As consequências foram severas e servem de alerta:

- Financeiras e Jurídicas: A Equifax foi forçada a pagar um acordo de aproximadamente US$ 700 milhões para encerrar investigações e compensar as vítimas, além de enfrentar inúmeros processos judiciais.
- Reputação: A confiança na marca, cujo negócio principal é a gestão de dados de crédito, foi profundamente abalada, causando um dano de longo prazo à sua imagem e valor de mercado.

A comparação evidencia que a negligência com a segurança digital, como a falta de atualização de sistemas (caso da Equifax) ou a falha na anonimização (caso da Fintech), pode levar a desastres corporativos de grande escala.

3. Plano de Ação Essencial para a Fintech

Um plano de recuperação eficaz deve ser estruturado em três áreas principais para mitigar os danos, cumprir a lei e reconstruir a confiança.

a) Ações de Prevenção e Segurança (Para Evitar Novos Incidentes):

- Segurança Técnica: Realizar uma auditoria completa para identificar e corrigir a falha que originou o vazamento. Implementar criptografia robusta para os dados armazenados e em trânsito, e adotar um sistema de monitoramento de segurança contínuo para detectar atividades suspeitas em tempo real.

- Políticas Internas: Desenvolver uma política de minimização de dados, assegurando que apenas as informações estritamente necessárias para a operação sejam coletadas. Além disso, é crucial revisar as permissões de acesso dos colaboradores, garantindo que sigam o princípio do menor privilégio.

b) Ações de Comunicação (Para Restabelecer a Confiança):

- Transparência e Suporte: Comunicar o incidente a todos os clientes afetados de forma clara e objetiva, detalhando os dados expostos e os riscos envolvidos. É fundamental oferecer, gratuitamente, serviços de monitoramento de crédito e identidade para proteger as vítimas de possíveis fraudes.
- Canais de Atendimento: Criar uma central de atendimento exclusiva para esclarecer dúvidas e orientar os clientes sobre como proceder para se protegerem.

c) Ações de Conformidade (Para Cumprir a LGPD):

- Comunicação com a ANPD: Notificar oficialmente a Autoridade Nacional de Proteção de Dados sobre o incidente, detalhando as causas e as medidas de contenção adotadas.
- Adequação aos Direitos dos Titulares: Implementar processos claros para que os clientes possam exercer seus direitos, como solicitar o acesso, a correção ou a eliminação de seus dados pessoais.
- Cultura de Privacidade: Investir em treinamento contínuo para todos os funcionários, disseminando a importância da proteção de dados como um valor fundamental da empresa.