IPACOM
Instituto Paranaense de Compliance

Guia 04
LGPD x Mercado Financeiro

IPACOM
Instituto Paranaense de Compliance

Este guia foi elaborado pelos membros do Grupo de Trabalho de LGPD do Instituto Paranaense de Compliance (IPACOM)

Elaboração
Caroline Fernandes Luiz
Laercio Almeida Junior
Marcos Goedert Melo
Mariana Fischer

Coordenação
Letícia Sugai

IPACOM
Instituto Paranaense de Compliance

Sistema Financeiro

- O Banco Central define o sistema financeiro como o ‘’conjunto de instituições financeiras e instrumentos financeiros que visam transferir recursos dos agentes econômicos (pessoas, empresas, governo) superavitários para os deficitários’’.
- Setor bastante afetado pela LGPD pois os dados dos clientes são fundamentais para a operação de diversos negócios.
- Por outro lado, é um mercado mais avançado em questão de adequação a LGPD devido ser o setor que mais investe em tecnologia e segurança da informação e já atende uma série de regulamentações.


Fintechs
Mercado monetário
Instituições de câmbio
Sistema Financeiro
Mercado de Seguros
Mercado de Capitais
Mercado de Crédito

O setor financeiro lida com dados pessoais extremamente importantes, tais como:

- Nome;
- CPF;
- Perfil de crédito;
- Ativos e dívidas do indivíduo.

necessitam de uma proteção maior por parte do Estado, pois são questões que interferem diretamente na economia e na vida do cidadão.

IPACOM
Instituto Paranaense de Compliance

LGPD destaca dois pontos indispensáveis para o mercado financeiro:

TRANSPARÊNCIA
clareza de informações sobre o tratamento de cada dado coletado.

CONSENTIMENTO
a devida autorização para o uso dos dados coletados.

IPACOM
Instituto Paranaense de Compliance

Bases legais mais relevantes no mercado financeiro:

- consentimento do titular dos dados pessoais;

- cumprimento de obrigação legal ou regulatória pelo controlador dos dados;

- relação contratual com o titular dos dados;
- para o exercício de direitos em processos judiciais, administrativos ou arbitrais;
- quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular;

- para proteger crédito, inclusive nos termos de legislações que tratem do tema.

O impacto para o mercado financeiro também está ligado com a consulta à base de terceiros, e transparência dos critérios de formação de score de crédito.

- Em relação à gestão de risco nas operações financeiras, a análise de dados é essencial para compreender o comportamento do consumidor e identificar de forma mais precisa potenciais fraudadores. Mas como é possível fazer isso sem ferir os direitos do titular?

BASE LEGAL

Legítimo interesse em evitar fraudes

Não é permitido usar essas informações para qualquer outra finalidade que não esteja amparada em uma das bases legais previstas na LGPD.

Regulamentação e fiscalização

CVM

Comissão de Valores Mobiliários - Instrução 358/02, buscou mostrar a necessidade de divulgação e o uso de informações sobre ato ou fato relevante, com o objetivo de se evitar que dados mantidos em sigilo possa afetar os investidores.

COAF

Estado vem tomando várias iniciativas que visam cruzar dados pessoais e financeiros para uma política mais eficiente contra lavagem de dinheiro e financiamento do terrorismo. Conselho de Controle de Atividades Financeiras auxilia nisso com a identificação de análise de ações suspeitas de atividades ilícitas.

IPACOM
Instituto Paranaense de Compliance

Regulamentação e fiscalização

BACEN

(Banco Central) - Em 2018, publicou a resolução 4.658, como define seu artigo 1º, sobre "a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

(Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais) - No início de agosto de 2016 publicou um guia que orienta as instituições na implementação de programa de cibersegurança.

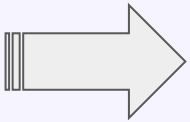
ANBIMA

Regulamentação e fiscalização

FEBRABAN

(Federação Brasileira de Bancos) - Em 2019, lançou um guia específico para o setor bancário de implementação da LGPD.

Também há algumas outras normas que protegem o direito à privacidade através da preservação da confidencialidade e sigilo, como a Lei do Sigilo Bancário, Lei de Lavagem de Dinheiro, e também o Código do Consumidor e o Código Penal que representam instrumentos importantes de proteção neste cenário.



Devem ser interpretadas e aplicadas considerando a proteção dos dados pessoais estabelecida pela LGPD.

IPACOM
Instituto Paranaense de Compliance

Importância das empresas atuantes do mercado financeiro se adequarem a LGPD

- Consequências legais do não cumprimento dessa legislação vão de multas e até mesmo a suspensão parcial ou total das suas atividades. Fora isso, também responde judicialmente outras violações previstas em lei.

- Tais penalidades financeiras resultam em danos à reputação e confiança dos consumidores. A notoriedade no mercado e nas relações com os clientes é um recurso essencial no mundo financeiro e precisa ser preservada.

- Manter um processamento dos dados de maneira transparente e com prioridade à segurança dos titulares deve ser incorporado às empresas. Para isso, a estruturação da área de dados deve ser voltada sobre o tema e ampliada a capacidade de atender ao direito dos clientes.

IPACOM
Instituto Paranaense de Compliance

Riscos Cibernéticos | Gestão

- O risco cibernético pode ser gerenciado, mas não pode ser eliminado.
- Cyber-Risk tem uma posição permanente dentre a gestão de riscos da organização.
- O risco cibernético é técnico por natureza, mas deve ser administrado em nível econômico.
- O gerenciamento de riscos cibernéticos envolve toda a organização, não apenas a TI.

4 opções de tratamento do risco

Evitar

Mitigar

Transferir

Aceitar

IPACOM
Instituto Paranaense de Compliance

Riscos Cibernéticos | Mitigação vs Transferência
Complementos não Alternativas

Mitigação

- Responsável: TI - Segurança
- Custo estimado: 5% -6% do orçamento de TI
- Impacto: reduzir a frequência de incidentes e em muitas vezes a severidade

Transferencia

- Responsável: Gestão de Riscos / Tesouraria
- Custo estimado: Depende do tipo de negócio
- Impacto: redução de perdas relacionadas a um incidente

Processos
Políticas de Segurança Cibernética
Plano de Resposta a Incidentes
Controles
Segurança Física

Práticas
Acompanhar novas ameaças
Gerenciamento de Fornecedores
Treinamento
Testes de Segurança

Tecnologia
Segurança de Aplicações
Segurança de Dados
Segurança de Rede
Segurança Operacional
Ferramentas e Sistemas

SEGURO

{ PROTEÇÃO EMPRESARIAL }

Ransomware Attack

Ransomware é um software malicioso que infecta seu computador e exibe mensagens exigindo o pagamento de uma taxa para fazer o sistema voltar a funcionar. Essa classe de malware é um esquema de lucro criminoso, que pode ser instalado por meio de links enganosos em uma mensagem de e-mail, mensagens instantâneas ou sites.

No Q4 de 2019, o tempo médio de recuperação de empresas que foram impactadas por esse tipo de incidente aumentaram para 16.2 dias de 12.1 dias na Q3 de 2019.

Average number of days a ransomware incident lasts.

Coveware Q4 2019 Ransomware Marketplace report


Cyber Liability | Garantias da Apólice
Indenizações e Acordos
Custos de Notificação e Monitoramento
Custos para Restauração de Dados e Sistemas
Custos de Gerenciamento de Imagem Pessoal e da Sociedade
Lucros cessantes por interrupção de rede
Custos de Defesa âmbito Administrativo
Multas
Extorsão
Custos de Defesa
Responsabilidade por Dados Pessoais ou Corporativos de Terceiros
Responsabilidade por Subcontratadas
VIOLAÇÃO
RECLAMAÇÃO DE TERCEIROS

Ataques cibernéticos a instituições financeiras têm aumento de 238%

Terceira edição do relatório anual da VMware “Modern Bank Heists” relata crescimento de ransomware, fraudes em transferências eletrônicas e island hopping a empresas do setor.

Os ataques de ransomware contra o setor financeiro aumentaram em nove vezes no mesmo período, de acordo com dados do estudo.27% de todos os ataques cibernéticos de 2020, até agora, foram direcionados aos setores de saúde ou financeiro.

Principais resultados da pesquisa

80% das instituições financeiras pesquisadas relataram um aumento de ataques cibernéticos nos últimos 12 meses – um crescimento de 13% em relação à 2019.

82% disseram que os cibercriminosos se tornaram mais sofisticados nos últimos 12 meses.

64% dos participantes relataram um aumento de 17% no número de tentativas de transferências eletrônicas fraudulentas nos últimos 12 meses, em relação à 2019.

33% das instituições financeiras disseram ter encontrado ao menos um ataque utilizando “island hopping” (em que cadeias de suprimentos e parceiros são obrigados a atingir a instituição financeira principal) nos últimos 12 meses.

Fonte: https://inforchannel.com.br/vmware-aponta-aumento-de-238-nos-ataques-ciberneticos-a-instituicoes-financeiras/

IPACOM
Instituto Paranaense de Compliance

Guia 04
LGPD x Mercado Financeiro

Elaboração
Caroline Fernandes Luiz
Laercio Almeida Junior
Marcos Goedert Melo
Mariana Fischer

Coordenação
Letícia Sugai