Executive REPORT
NEGÓCIOS & TIC – TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

LGPD NO SETOR FINANCEIRO

EXECUTIVE REPORT - EXPEDIENTE

DIREÇÃO E EDIÇÃO EXECUTIVA
Graça Sermoud
gsermoud@conteudoeditorial.com.br

DIREÇÃO DE MARKETING
Sérgio Sermoud
ssermoud@conteudoeditorial.com.br

DESIGN
Rafael Lisboa
rlisboa@conteudoeditorial.com.br

EDITORA
Léia Machado
lmachado@conteudoeditorial.com.br

REDAÇÃO / REVISÃO
Paula Zaidan
pzaidan@conteudoeditorial.com.br

LGPD CORROBORA A TRANSFORMAÇÃO DOS NEGÓCIOS NO SETOR FINANCEIRO

Estudos e análises de mercado revelam: o ecossistema financeiro está à frente de outros mercados quando se trata de implementar o plano de ação para a LGPD. A razão é simples. Além de ser o setor que mais investe em tecnologia e segurança da informação, tradicionalmente atende uma série de regulamentações.

Esse setor ainda vive dias de profunda transformação, dada a proximidade com o modelo de Open Banking, que a partir de 2020 mudará a maneira de o segmento se relacionar com o cliente. Nesse aspecto, a Lei Geral de Proteção de Dados é, por unanimidade dos CISOs, a alavanca propulsora para a mudança, uma vez que o consumidor passa a ser o dono do dado e ele decidirá o nível de segurança e quais serviços usufruir de toda a cadeia financeira.

Especialmente na indústria financeira, a LGPD traz dois pontos fundamentais a serem observados pelas instituições: transparência e consentimento. O primeiro ponto se refere à clareza de informações sobre todo tratamento que será aplicado ao dado coletado e consentimento trata da autorização do uso desses dados. É mapear os fluxos e identificar a tomada de consentimento nas interações com clientes, e verificar se a autorização por parte do usuário foi realizada de acordo com as novas normativas.

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.

O comprometimento desses recursos pode significar não apenas perdas para o banco envolvido, mas também para todo o mercado por causa do risco sistêmico que um incidente pode causar. Logo, investir na segurança cibernética deixou de ser opção para empresas, sendo quesito indispensável para a própria sobrevivência da corporação, já que os ataques cibernéticos geram diversas perdas financeiras e envolvem diminuição de receita e prejuízos a marca e reputação. Há um custo social elevado a ser pago que é o da reconstrução da confiança dos clientes.

A KPMG aponta que a agenda regulatória será intensa para o sistema financeiro este ano, principalmente, para as grandes empresas do mercado, com previsão de aumento de capital para aqueles que preveem crescimento de ativos. O levantamento aponta ainda que esse novo cenário possibilita que outras instituições possam migrar do modelo de serviços financeiros para um de serviços tecnológicos.

De acordo com a pesquisa, os prestadores de serviços financeiros devem manter a governança e os controles dentro da uma estrutura de gestão de risco para a fluidez da agenda. Questões sobre fortalecimento das práticas de gestão de risco e, principalmente, tecnologia de informação e governança de dados, segundo o estudo, são os pontos de maior preocupação, pois sem uma regulamentação de privacidade o mercado continuará com uma lacuna nessas questões.

Existe ainda uma expectativa com relação aos trabalhos da Agência Nacional de Proteção de Dados, que foi criada pela Medida Provisória 869/18, mas que ainda não saiu do papel. Além disso, o Banco Central publicou o ano passado a Resolução 4.658. Essa norma, referente à política de segurança cibernética e requisitos para contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, entrará em vigor em 2021 gerando obrigações adicionais às empresas reguladas junto ao BC.

CONFIANÇA E PROTEÇÃO DE DADOS NA ESTEIRA DA LGPD

Diante de um cenário regulatório exigente, as instituições financeiras brasileiras estão em um nível maior de maturidade de segurança de dados se comparado aos outros setores, a ponto de o consumidor confiar em fornecer seus dados pessoais aos bancos. É o que revela recente estudo da Serasa Experian.

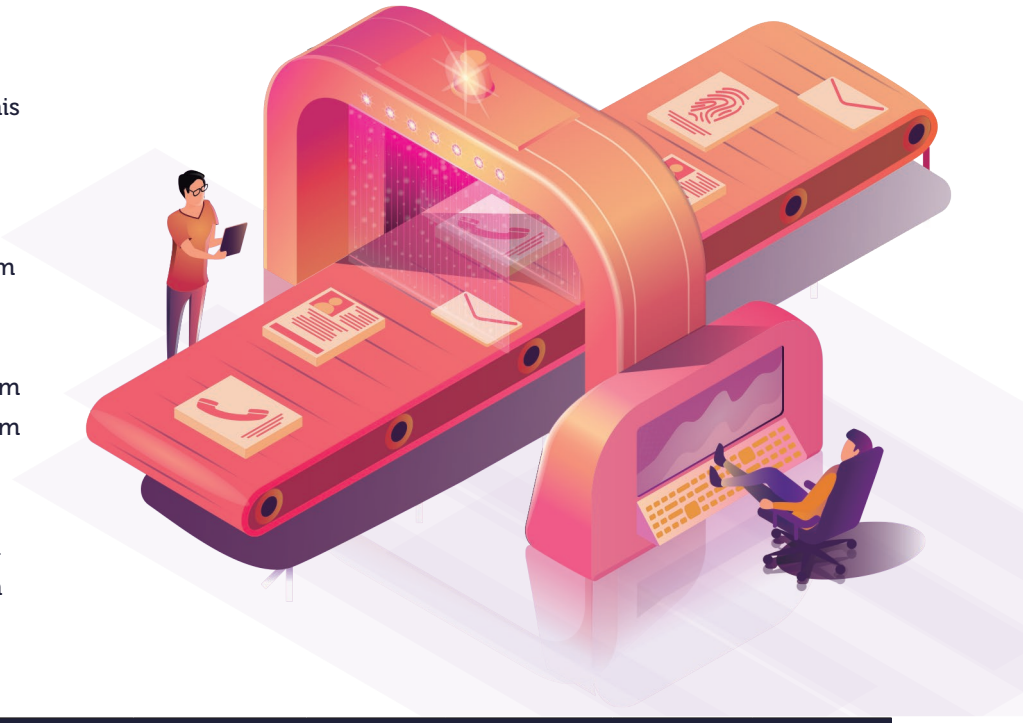
PRIVACIDADE, O CALCANHAR DE AQUILIS DOS BANCOS

"Os dez principais desafios regulatórios" (Ten Key regulatory challenges of 2019, em inglês) mapeou os assuntos que afetarão as instituições financeiras este ano:

1. privacidade de dados,
2. crimes financeiros,
3. controles e governanças de riscos,
4. processos de compliance,
5. gestão de crédito,
6. segurança cibernética,
7. ética e conduta,
8. proteção a consumidores,
9. proteção ao capital,
10. liquidez.

Fonte: KPMG

Cinco em dez brasileiros confiam mais em instituições financeiras, como bancos e seguradoras, para compartilhar os dados. A pesquisa aponta que as instituições financeiras passam mais confiança quando comparadas com provedores de meios de pagamento e provedores de tecnologia. Em números, 46% dos brasileiros preferem compartilhar dados com os bancos. Em segundo, estão os provedores de meios de pagamento com 25% e, em terceiro, os provedores de tecnologia com 10%.



SEGMENTOS MAIS CONFIÁVEIS PARA COMPARTILHAR DADOS PESSOAIS

(NEGÓCIOS LISTADOS PELA PESQUISA POR REGIÕES/PAÍSES)

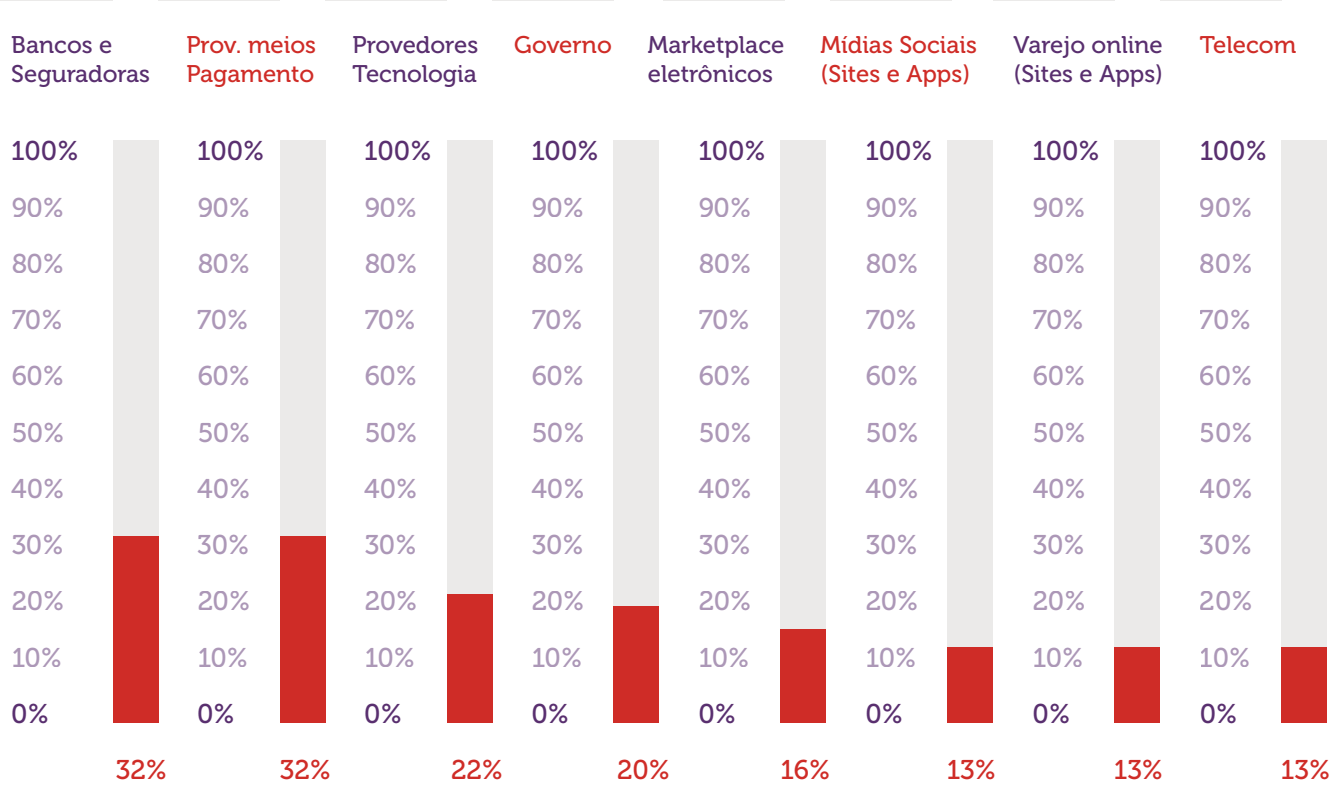
SEGMENTO	BRASIL	GLOBAL	ESTADOS UNIDOS	REINO UNIDO	COLÔMBIA	EMEA*	APAC*
Bancos e Seguradoras	46%	37%	42%	41%	54%	37%	33%
Provedores de meios de pagamento	25%	18%	21%	22%	18%	17%	17%
Provedores de Tecnologia	10%	6%	5%	5%	6%	3%	7%
Órgaãos governamentais	9%	27%	15%	20%	11%	34%	28%
Mídias Sociais (Sites e Apps)	5%	4%	4%	3%	1%	2%	5%
Marketplaces de eletrônicos e telefonia mobile	2%	4%	5%	5%	3%	4%	4%
Lojas de Varejo online (sites e aplicativos)	2%	2%	2%	4%	2%	2%	2%
Empresas de telecomunicação	2%	3%	5%	1%	4%	2%	3%

Fonte: experian

*APAC: Austrália, China, Hong Kong , Índia, Indonésia, japão, Malásia, Nova Zelândia, Singapura, Tailândia e Vietnã.

*EMEA: África do Sul, Alemanha, Áustria, Espanha, França e Holanda/Países Baixos.

O levantamento também avaliou como o consumidor lida com coleta, uso e armazenamento de seus dados pessoais por parte das empresas. Nesse contexto, o setor financeiro novamente ficou em evidência. 32% dos brasileiros disseram que "confiam totalmente" nas instituições financeiras. O mesmo percentual se repete para meios de pagamento, posicionando esses segmentos no Brasil à frente dos demais países. ◁◁



COMPETIÇÃO SAUDÁVEL: O QUE É DESAFIO TORNA-SE OPORTUNIDADE

Cultura, pequenos ajustes e segurança como serviço são os grandes desafios enfrentados pelo mercado financeiro, com o apoio de tecnologias disruptivas, para implementar a LGPD

O setor financeiro é um dos mais avançados do ponto de vista da LGPD, dado o rigor no cumprimento de normas, leis e regulamentações. Foi feito um levantamento a pedido da FEBRABAN com o escritório Tozzini Freire. Um dos aspectos identificados foi que os bancos fazem 20 tipos diferentes de tratamento de dados (cadastro, consulta, abertura de contas, verificação para envio ao Banco Central, etc.). E, ainda, as instituições financeiras estão sujeitas a 162 leis e 197 decretos. Além disso, muitos dos bancos já seguem legislações internacionais de dados pessoais, uma vez que fazem negócios com outras instituições fora do País.

"Por isso, a LGPD é só mais um ajuste. Não uma questão de desespero para o ecossistema e nem para as fintechs", aponta Adriano Mendes, advogado especialista em Proteção de Dados e Sócio da Assis e Mendes Advogados. Mendes observa que o desafio agora para os bancos é a conscientização, criar uma cultura, uma vez que a resolução do Banco Central 4,658/2018 (que dispõe 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) contribuiu para aumentar os controles. "Os ajustes necessários são menos complexos se comparados com outros setores, embora sejam altamente rígidos".

No entanto, o advogado avalia que existem algumas práticas de rotina nos bancos contraditórias à LGPD. "De acordo com a Lei Geral de Proteção de Dados, é necessário fazer uma análise prévia do cliente. O banco também faz isso num título de capitalização ou pagamento de seguro e se a pessoa que o cliente indica como beneficiário não está ligada exatamente ao banco, isso impacta em uma análise de terceiros e, nesse caso, a instituição financeira terá que justificar porque está realizando esse tipo de operação. Nesse caso, o banco terá que justificar, uma vez que ninguém pensou nisso antes da LGPD. E agora terão que fazer o tratamento caso a caso".

Ainda do ponto de vista legal, Mendes comenta que, sobre os casos de ataques, a maior novidade é notificar os envolvidos. No caso de uma vulnerabilidade que comprometa uma senha, será informado ao usuário que os dados dele estão vulneráveis. Por exemplo, é comum receber uma conta de água, luz ou telefone enviada para a pessoa errada. "No caso dos bancos, segurança e proteção de dados sempre foi uma preocupação e isso tende a aumentar".

PORTABILIDADE E TRANSPARÊNCIA: VEM AÍ NOVOS SERVIÇOS

O Open Banking, um estudo do BACEN permitindo que terceiros possam acessar a sua conta e tomar ações, garantirá o direito à portabilidade e transparência e isso terá um grande impacto no mercado financeiro. O Open Banking exige um cuidado diferenciado de validação jurídica do que existe hoje (que seus dados e a sua conta são pessoais e intransferíveis).

"Diante disso, os bancos terão que controlar de forma rígida quem está fazendo aquele acesso. Hoje na LGPD tem a figura do controlador e operador. Se o banco é o controlador e tem um vazamento por uma fintech, ele pode pagar uma multa em decorrência daquele incidente. Na dúvida, ambos estarão envolvidos nessa multa. Mas as fintechs já são uma realidade, nos Estados Unidos e na Europa elas já tomaram conta do mercado".

Por isso, segundo Mendes, um dos grandes impactos da LGPD será nas fintechs. Muito do que elas têm feito é automatizar e criar algoritmos inteligentes que dispensam análise por humanos, o que vai contra a LGPD, que exige contato com um humano, uma vez que serão emitidos os relatórios de conformidade. Essa revisão por humano não significa necessariamente que seja feita por uma pessoa e sim que aquela equação matemática foi vista por alguém e está conforme. Dessa forma, as fintechs farão essa análise uma única vez".

Segundo Mendes, as ferramentas da Fortinet ajudarão as instituições financeiras na clareza de onde estão as informações e o que podem fazer a partir desse cenário. "As provedoras de tecnologia ajudarão na garantia de que nenhuma informação saia da instituição e que haja mais transparência naquilo que aconteceu de forma automatizada. Com o uso do conceito do Fabric, da Fortinet, que utiliza Inteligência Artificial e Machine Learning, caso haja um incidente com os dados do cliente, será possível detectar se aconteceu dentro da instituição ou em terceiros".

No caso do Open Banking, onde o cliente decide se fornecerá seus dados ou não, e o nível de segurança que quer ter, a agilidade no tempo de resposta aos vazamentos de dados é fundamental para que os bancos e todo o ecossistema financeiro tenha uma resposta rápida em consonância com os requisitos da LGPD.

"De nada adianta ter todo o processo elaborado com assessoria jurídica se a proteção de dados tem uma vulnerabilidade e gera um vazamento. Por isso, o cliente deve levantar a bandeira jurídica junto com a garantia de que a infraestrutura esteja preparada para a proteção de dados. Isso é possível com o Security Fabric, o que garante três pontos fundamentais em consonância com a LGPD: visibilidade, integração e automação", diz Alexandre Bonatti, diretor de Engenharia de Sistemas da Fortinet.

1. VISIBILIDADE – Capacidade de, em tempo real, por meio de um dashboard, controlar tudo que está acontecendo na sua infraestrutura, seja ela on premise ou multicloud.

2. INTEGRAÇÃO – Do ponto de vista do open banking é fundamental integrar todas as soluções de segurança, uma vez que os bancos têm suas linguagens próprias. O Security Fabric segue conceito de open, permitindo via APIs a integração com terceiros, chamado um ecossistema aberto. Independente se o vendor é A ou B é possível ter visão geral da infra.

3. AUTOMAÇÃO – Visão e tempo de resposta. O problema não é ser atacado, mas sim o tempo de resposta ao ataque. Estamos lidando com máquinas e não há como o humano resolver no mesmo tempo de resposta. Portanto, a automação permite uma análise profunda da ameaça, mecanismo de alerta e uma ação. Essa ação quem define é o próprio cliente. O Fabric permite o compartilhamento da IA de ameaças. ◁◁

BANCO VOTORANTIM:
AJUSTES NAS CONTAS DA LGPD

A instituição financeira desenvolveu uma suíte que centraliza os dados para facilitar a gestão das informações, minimizar as vulnerabilidades e permitir uma visão única por meio de um painel de controle acessado pelo DPO global

Familiarizado com a GDPR, o Banco Votorantim iniciou no ano passado o seu plano de ação para cumprir a LGPD. Para tanto, constituiu um grupo de trabalho multidisciplinar (TI, jurídico, segurança, entre outras áreas) que reporta as iniciativas desenvolvidas aos diretores executivos da instituição. Paralelamente, a instituição tem cumprido uma extensa agenda com a participação de seus colaboradores em congressos, treinamento, além da conquista de diversas certificações baseadas nas práticas europeias. E, ainda, criou uma suíte com uma base única de dados.

PROTEÇÃO DE DADOS: DO ON PREMISE AO CLOUD

Cultura ágil, uso de novas plataformas digitais e parcerias com as fintechs para atender a jornada de seus clientes. Esse é o DNA do Banco Votorantim e a proteção de dados, seja no ambiente on premise ou cloud, é requisito fundamental para quem enxerga o seu usuário no centro do negócio.

Para tanto, Mattos explica que o banco criou um arcabouço único de sua base de dados, capaz de mapear todos os cadastros dos clientes. "Assim, desenvolvemos uma suíte para realizar a gestão da LGPD, envolvendo requisitos de opt-in, opt-out, enquadramento, entre outros aspectos que cobrem todo o ciclo de vida do dado de forma centralizada".

Segundo Mattos, o projeto será concluído no final de 2019 e permitirá, por exemplo, a identificação dos dados compartilhados, quais estão armazenados dentro de uma estação de trabalho, entre outras análises que garantirão uma visão única ao DPO global do banco por meio de um painel de controle. O próximo passo é a revisão dos contratos com terceiros sob a responsabilidade do jurídico do banco.

"Ainda teremos adequações porque as coisas estão um pouco nebulosas. Somente a partir da operação da ANPD será possível obter mais clareza sobre alguns itens bastante interpretativos no texto da LGPD", observa. ◁◁

"Hoje, o programa de implementação da LGPD está numa fase de ajustes tecnológicos e jurídicos. Estamos avaliando quais ferramentas serão implementadas para controlar o ciclo de vida do dado, analisando a questão dos opt--ins, o que impacta na gestão das informações dos clientes que solicitarem o esquecimento e assim harmonizar as regras da LGPD com as regulamentações exigidas pelo Banco Central", explica André Mattos, Head Data Analytics Corporate Systems do Banco Votorantim.

Do ponto de vista de ferramentas de segurança da informação, Mattos ressalta que não há uma solução única para estar em conformidade com a LGPD, mas é essencial orquestrar uma composição tecnológica calibrada. "Não existe bala de prata. Mitigar os ataques e vulnerabilidades continua sendo a nossa prioridade. O que mudou é que agora temos um balizador, a Lei Geral de Proteção de Dados". Por isso, o banco utiliza um arsenal capaz de minimizar os riscos, como as soluções da Fortinet. "Em nossas filiais, a infraestrutura de rede e telefonia é apoiada por uma suíte de segurança da Fortinet", diz Mattos.

HÁ 10 ANOS, O MAIOR E MAIS QUALIFICADO EVENTO DE LÍDERES DE SEGURANÇA DA INFORMAÇÃO DO BRASIL

AGUARDE SÃO PAULO!

» *29 E 30 DE OUTUBRO*

Hotel Transamérica

REALIZAÇÃO: SECURITY LEADERS 10 ANOS

APOIO: Security Report | Decision

FORTINET

Prepare-se para a LGPD, com o Fortinet Security Fabric

Amplo, Integrado e Automatizado

O Fortinet Security Fabric possibilita uma resposta única e centralizada para os desafios da LGPD. Com atuação abrangente no ecossistema corporativo, as respostas e ações contra às ameaças, serão dinâmicas e automatizadas.

www.fortinet.com