IDC VENDOR SPOTLIGHT
Patrocinado por: Kaspersky

Entendendo os impactos da LGPD com treinamento e conscientização

As empresas precisam ampliar seu entendimento sobre a Lei Geral de Proteção de Dados (LGPD) para assegurar que estejam cumprindo adequadamente seus requerimentos, evitando duras sanções sobre seus negócios.

Junho, 2021

Escrito por:
Luciano Ramos, Gerente de Pesquisa e Consultoria – IDC Brasil

I. Introdução

O mundo passa por um momento ímpar na sua história. O panorama global de enfrentamento dos reflexos da pandemia fez com que as organizações repensassem muito rapidamente as formas de engajar e interagir com seus clientes. O estudo *IDC Latin America COVID-19 Impact on IT Spending 2020* mostrou que os consumidores se adaptaram à nova realidade e mudaram seus hábitos. Para 52% deles, o volume de compras *online* cresceu, enquanto 45% dos respondentes apontaram que aulas e cursos *online* passaram a ser uma opção viável e interessante para seu desenvolvimento pessoal ou profissional.

Esses dados, portanto, mostram que os canais digitais assumiram um papel de protagonismo diante da crise, o que fez com que as empresas tivessem que habilitar e escalar essas capacidades em um curto espaço de tempo. Essas iniciativas, em grande parte dos casos, já estavam no *roadmap* de desenvolvimento das organizações; a crise atuou como um catalizador.

Diante desse cenário, as estratégias que tocam o *Customer Experience* (CX) foram priorizadas pelas empresas e continuam em foco. De acordo com o *IDC Predictions Brazil 2021*, 65% das empresas de médio e grande porte no país afirmam terem planos para dar maior ênfase a esse tema ao longo de 2021. Trata-se de um mercado que deve atingir US$ 1,4B já neste ano, o que representa um crescimento de 21,3% em relação a 2020.

EM DESTAQUE

DADO IMPORTANTE

No Brasil, 50% das empresas de grande porte encontram-se em estágios avançados de adequação à LGPD. Outros 31% têm ações em andamento.

VALE LEMBRAR

A Lei Geral de Proteção de Dados foi criada para proteger tanto dados físicos como digitais. Por isso, não se trata de uma iniciativa exclusiva da TI, mas da organização como um todo.

CX exige soluções que viabilizem o *Digital First* – abordagem estratégica que coloca os canais digitais em posição de destaque – e propiciem experiências personalizadas e maior automação. Para que isso seja possível, as empresas vêm aumentando consideravelmente a captação de dados de seus clientes nos últimos anos, criando estruturas que vão desde repositórios simples para lidar com dados pontuais, como o e-mail ou o telefone celular para envio de notificações, até soluções complexas como *Data Lakes* que somam informações de múltiplas fontes, como histórico de interações, navegação por *websites*, dados coletados de redes sociais, entre outros.

Lidar com esses dados pessoais se tornou um assunto importante; as pessoas têm direito à privacidade e precisam ter clareza de como seus dados são captados, para que finalidade serão utilizados e como serão processados, armazenados e, finalmente, descartados. Isso vai ao encontro do que é regido pela LGPD, lei voltada para proteção de dados pessoais, em vigor no Brasil desde setembro de 2018.

Sobre a LGPD

A Lei Geral de Proteção de Dados, conhecida por LGPD, tem o objetivo de garantir aos cidadãos brasileiros maior controle e transparência sobre o uso de seus dados pessoais. A lei unifica regras e determina caminhos para este tema, afetando todo o ciclo de vida dos dados em uma empresa. Apesar de estar em vigor desde 2018, uma série de adiamentos fez com que suas sanções sejam efetivamente aplicadas apenas a partir de agosto de 2021. Em paralelo a isso, houve também a definição e criação a Autoridade Nacional de Proteção de Dados (ANPD) que regulará sob as disposições da lei.

São várias as regras estabelecidas pela LGPD, mas podemos destacar 4 grandes tópicos:

- **Mapeamento e organização dos dados pessoais que a empresa mantém:** inclui também a categorização dos dados, incluindo aqueles considerados sensíveis e que precisam ter um tratamento mais rigoroso;
- **Monitoramento do ciclo de vida dos dados:** considera os dados pessoais que transitam na empresa, sendo necessário ter clareza sobre os processos que os utilizam, para quais finalidades e como acontece seu armazenamento e descarte;
- **Estabelecimento de uma política clara e práticas de governança:** dá as diretrizes para que os colaboradores da empresa saibam como atuar no dia a dia com dados pessoais, orientando-os também sobre como assegurar que suas práticas são seguras e como torná-los menos vulneráveis;
- **Definição de um responsável pela LGPD na organização:** define a necessidade de um DPO (do inglês, *Data Protection Officer* – responsável pela proteção de dados), que é o responsável por cuidar dos controles relacionados à LGPD e a prestar quaisquer esclarecimentos que se façam necessários diante de uma auditoria ou de um evento adverso.

II. O Estado da LGPD nas Empresas no Brasil

Ainda que, como destacado, a lei já esteja em vigor, muitas empresas no Brasil seguem organizando e conduzindo iniciativas para adequar seus processos e governança de acordo com as disposições estabelecidas pela LGPD. Segundo o estudo *IDC Brazil Security Leaders 2020*, apenas 50% das empresas entrevistadas afirmaram estar em estágios avançados de adequação. Outros 31% indicaram que têm ações em andamento e, portanto, precisam acelerar as atividades para colocar seus negócios em linha com a regulação.

É importante frisar que a LGPD cobre a proteção dos dados pessoais sejam digitais ou físicos. Ou seja, as organizações também precisam ficar atentas aos processos em que há entrada de dados por formulários de papel, bem como controlar melhor o manuseio e a saída física das informações em documentos impressos em geral. O arquivamento e o descarte de informações armazenadas em meios físicos precisam ser tratados na política de proteção de dados da empresa e nas normas relacionadas, de forma que seja possível rastrear e validar esses procedimentos.

FIGURA 1: ***Estágio de Adequação para a LGPD no Brasil***

Fonte: IDC Brazil Security Leaders, Novembro 2020.

Principais Desafios

Sabemos como pode ser complexo fazer grandes mudanças dentro das empresas. Por vezes, estamos falando de processos que há anos fazem as coisas da mesma forma, sem um maior nível de controle ou de visibilidade. Em outros casos, nos referimos a dezenas de sistemas legados que impõem obstáculos para entender plenamente seu fluxo de informações e as integrações entre eles. E, sem dúvida, há a necessidade de envolver e capacitar as pessoas para as mudanças que estão por vir; quando os colaboradores têm clareza sobre os motivos e benefícios da mudança, seu engajamento aumenta e há abertura para estabelecer um novo *modus operandi*.

Com a LGPD, isso não é diferente. Quando perguntados sobre os principais impactos que a lei geral de proteção de dados traz para suas empresas, 67% dos executivos apontam para o desafio do mapeamento dos dados da organização e seu controle efetivo – segundo o estudo *IDC Brazil Security Leaders 2020*. Por esse motivo, as empresas precisam:

- Lançar mão de uma investigação detalhada sobre processos que gerem, processem ou armazenem dados físicos (não digitais), para entender pessoas e responsabilidades, fluxos por onde esses dados passam e onde se integram a processos digitais, certificando-se se há ou não descarte do dado físico após sua integração. Tal

investigação precisa ser documentada e alinhada com todas as áreas envolvidas em cada um dos processos manuais mapeados.

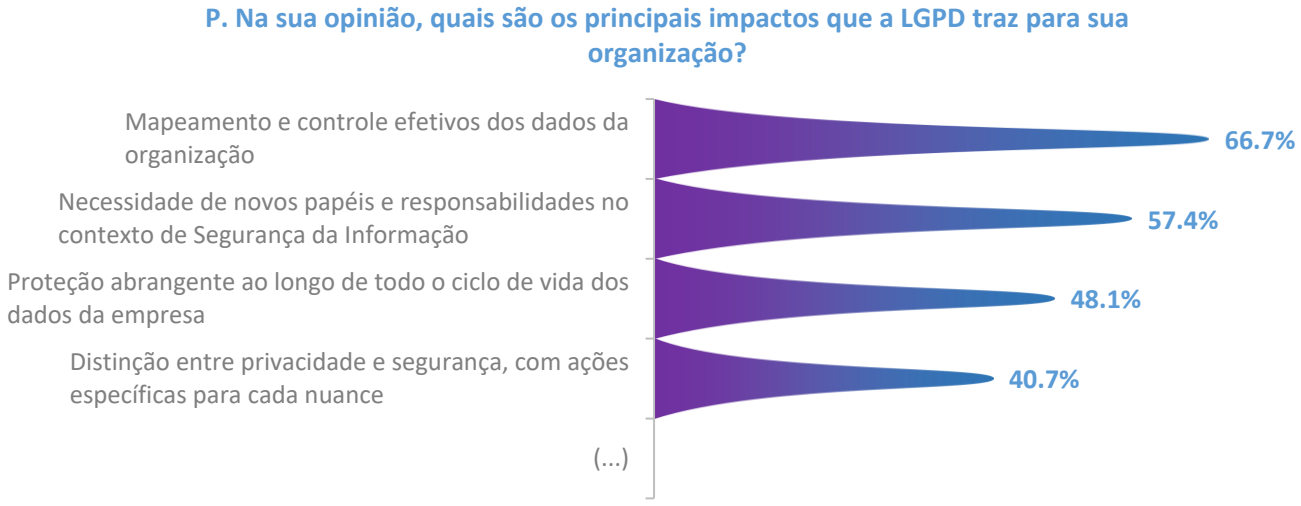
» Diante do volume, do dinamismo e da complexidade dos dados digitais, considerar a utilização de soluções de TI que consigam analisar e classificar o tráfego de informações entre os diversos ambientes e sistemas da organização, criando assim um mapa abrangente que detalha origem e destino, bem como atores e ações sobre cada dado analisado.

Os dados digitais representam hoje um dos principais ativos de negócio dentro das companhias, suportando processos e tomadas de decisões. Por isso, é cada vez mais comum que as organizações agreguem capacidades de segurança – como criptografia, segmentação de ambientes e redes, entre outras – para protegê-los, minimizando riscos de vazamentos e, consequentemente, punições pela lei.

Não obstante, muitas empresas esquecem ou ignoram que a LGPD não é só para dados digitais. Por cobrir também os dados pessoas em meios físicos, a LGPD afeta múltiplas áreas além da TI e da segurança da informação (SI) – marketing, operações, vendas, entre outras. Gestores e colaboradores são afetados e precisam ter o comprometimento com o processo de adequação, independente do ramo de atuação ou do porte da companhia. Faz-se necessário, portanto, envolvê-los e educá-los sobre as disposições da lei, de forma que entendam o porquê das mudanças e possam contribuir durante jornada e manter-se alinhados à lei de forma permanente.

Esse também é um ponto central dos impactos que a LGPD impõe sobre as empresas, segundo estudo da IDC; 57% delas apontam o desafio de esclarecer os novos papéis e responsabilidades no contexto de segurança da informação. Por isso, treinar toda a organização pode ser chave para uma adequação bem-sucedida que resultará na manutenção de práticas sempre alinhadas à lei, à política da companhia e demais normas internas.

FIGURA 2: ***Percepção dos Impactos da LGPD nas Organizações***



Fonte: IDC Brazil Security Leaders, Novembro 2020

Vale ressaltar que, ainda que as soluções de TI possam ajudar na identificação, mapeamento e controle de informações em meio digital, não há uma solução ou produto que resolva a adequação à LGPD em toda sua extensão – em especial, a parte de conhecimento e conscientização das pessoas dentro da empresa.

Impacto dos Ataques Cibernéticos

Outro aspecto importante que toca a proteção de dados pessoais tem relação com os riscos relacionados aos ataques cibernéticos. Conforme a pandemia da COVID-19 progredia durante o primeiro trimestre de 2020 e as empresas adotavam o *home office* e a educação remota, quase três milhões de ataques cibernéticos ocorreram na América Latina. No mesmo período, o número de vírus de computador aumentou 131% em comparação ao ano anterior, acompanhando o aumento do tráfego da *web* na maioria das áreas urbanas.

Ao longo de 2020, Brasil e Venezuela foram os dois países com a maior incidência de ataques de *phishing* na região, com 19,9% e 16,8%, respectivamente. Esses ataques tornaram os usuários suscetíveis a vários tipos de outros ataques mais violentos, incluindo *ransomware*, que, após a infecção, bloqueia o acesso aos dados até que um pagamento seja recebido em troca. O Brasil também foi o país com mais ataques de *ransomware*, com quase 46,7% dos usuários infectados, seguido pelo México, com aproximadamente 22,6%, e pela Colômbia com mais de 8%.[1]

Isso evidencia a necessidade de conjugar adequação de processos e soluções avançadas de segurança, que permitam não somente detecção de ameaças modernas, mas também que gerem um fluxo de resposta a incidentes.

III. Benefícios Esperados com os Efeitos da LGPD

O advento da LGPD no Brasil acompanha um movimento global de conscientização sobre o direito à privacidade dos indivíduos. Para as pessoas de modo geral, isso permitirá maior entendimento e controle sobre quem tem acesso às suas informações e como as utilizarão, evitando assim abusos e mal uso desses dados. Cada cidadão poderá pedir, a qualquer momento, a prestação de contas sobre os dados que cada empresa mantém sobre ele, bem como solicitar sua exclusão e consequente eliminação dos respectivos dados em domínio da empresa – esteja ele em meio físico ou digital.

Ainda sob a perspectiva do indivíduo, a lei de proteção de dados pessoais abre espaço para uma maior conscientização das pessoas sobre o valor e criticidade desse tipo de dado. Atualmente, grande parte das pessoas não dá atenção para como as empresas lidam com suas informações – embora seja frequente a reclamação sobre contatos e serviços indesejados oferecidos com base em dados que foram indevidamente compartilhados entre diferentes prestadores de serviços.

De forma análoga, as pessoas em geral também não se dão conta que seus dados podem ser igualmente expostos a cibercrimosos – elas pensam, equivocamente, que seu dado individual não tem valor e, portanto, acabam não se preocupando com sua proteção. A LGPD traz um grande benefício ao motivar os cidadãos a entender mais claramente os impactos deste grande conjunto de dados – os seus somados aos de outras pessoas – quando mal utilizados, o que muda sua postura diante do seu compartilhamento e autorização de uso, gerando um efeito positivo que tende a se propagar de forma exponencial.

Olhando sob o prisma de uma empresa e seus vários colaboradores, para que essa percepção e conscientização permeiem a cultura da empresa, não basta contar com o amadurecimento individual comentado anteriormente. É preciso estabelecer programas de educação que toquem os colaboradores e possam evidenciar:

- A importância da lei e suas implicações sobre a cultura da empresa;

[1] Fonte: Statista, 2020.

- O impacto nos processos de negócio e a necessidade de preparação para adequação;
- Práticas para manter o alinhamento constante e o mapeamento de novos fluxos de informação;
- Papéis e responsabilidades associadas ao cumprimento da LGPD.

Um currículo bem elaborado de treinamento pode não apenas simplificar e acelerar o processo de adequação, mas também proporcionar um maior amadurecimento da postura de segurança da organização como um todo.

De forma geral, as empresas têm desafios para treinar e capacitar seus funcionários. A LGPD, em especial, acentua esses obstáculos por tocar em temas que, por vezes, não faziam parte do dia a dia da maioria dos colaboradores. Por isso, contar com um parceiro especializado que tenha não apenas o domínio sobre a lei, mas também possua as dinâmicas e ferramentas necessárias para um engajamento efetivo pode ser essencial para o sucesso dessas iniciativas com resultados perenes.

IV. Perfil do Provedor – Kaspersky

Fundada em 1997, a Kaspersky Lab é uma empresa internacional especializada em segurança virtual. As soluções e serviços de segurança da Kaspersky são apoiadas em sua larga experiência e em capacidades de inteligência de ameaças, que protegem empresas e consumidores ao redor do globo.

Num cenário em constante mudança, a Kaspersky busca oferecer um portfólio abrangente que inclui proteção de *endpoints* e inúmeras soluções e serviços de segurança para combater ameaças digitais complexas e em constante evolução. São mais de 400 milhões de usuários em todo o mundo sob a proteção das tecnologias da Kaspersky Lab, e 270 mil clientes corporativos onde suas soluções ajudam a proteger seus ativos mais importantes.

Visando ajudar as empresas nas suas jornadas para adequação às regras trazidas pela LGPD, a Kaspersky estabeleceu um programa amplo de treinamento sobre *Security Awareness* que integra múltiplas plataformas e ferramentas para engajar diversos públicos dentro de organizações de todos os tamanhos. Cada uma das 3 etapas do programa lança mão de recursos específicos que têm como objetivo assegurar o aprendizado e sua aplicação em situações reais de negócio.

Kaspersky Automated Security Awareness Platform (ASAP)

Plataforma de aprendizado totalmente *online*, com conteúdo voltado para os temas de visibilidade e conscientização sobre a segurança da informação no ambiente corporativo – incluindo o tema da LGPD e seus impactos.

Podendo ser utilizada por empresas de todos os portes, desde as PMEs até as grandes *Enterprises*, a Kaspersky ASAP oferece suporte para todas as etapas da jornada de conscientização, desde o estabelecimento de metas até a avaliação de resultados usando relatórios e análises acionáveis.

A plataforma conta com recursos como definição simplificada de objetivos, caminhos de aprendizagem automatizados, exercícios práticos baseados em cenários da vida real, integrados com acompanhamento e auditoria que permitem que gestores acompanhem o progresso de suas equipes em tempo real, identificando *gaps* e oportunidades para acelerar a assimilação do conhecimento.

O conteúdo do programa é estruturado para apoiar a microaprendizagem, mantendo as sessões de treinamento focadas e curtas para fornecer altos níveis de retenção. Cada tópico de segurança é abordado por meio de uma

combinação de diferentes formatos de conteúdo, que vão desde elementos de treinamento até simulações de *phishing* e mensagens maliciosas.

Gamification e Dinâmicas Interativas

Para assegurar que o conhecimento está sendo assimilado pelas equipes, a Kaspersky desenvolveu um conjunto de dinâmicas interativas que colocam as pessoas diante de situações reais ligadas à segurança das informações para que possam aplicar seus aprendizados.

Em um formato que simula um jogo, os participantes precisam analisar cenários e ameaças para fazer as escolhas certas sobre o tipo de proteção que deverão empregar em cada etapa. As escolhas acertadas os levarão a avançar no jogo, enquanto as decisões erradas farão com que percam tempo e dinheiro.

A técnica de *gamification* é um recurso bastante eficaz para assegurar engajamento das equipes e uma experiência colaborativa de aprendizado. Cada equipe poderá comparar seus resultados com os demais times e, com isso, identificar mais rapidamente os pontos de atenção que precisam ser endereçados. A dinâmica completa conta com vários módulos, voltados para segmentos de mercado específicos e suas peculiaridades.

Kaspersky Expert Training

As ameaças estão em constante evolução. Por isso, é vital que os especialistas em segurança de TI mantenham suas habilidades atualizadas. O *Expert Training* da Kaspersky, voltado para o CISO (*Chief Information Security Officer*) e para os times de segurança, visa atingir esse objetivo apresentando estratégias eficazes de detecção e mitigação de ameaças.

Criados sobre uma plataforma de aprendizado *online*, os cursos especializados abordam tópicos avançados ao redor da prevenção e detecção de ameaças, especialmente os *malware*. Entre os temas estão a engenharia reversa de *software* maliciosos e as regras Yara (voltadas para descrição de famílias de *malware* e suas variações).

Desafios para a Kaspersky

Mesmo com o reconhecimento da importância dos treinamentos de segurança, muitas empresas deixam essas iniciativas em segundo plano. Por consequência, acabam por reagir mais lentamente diante das constantes mudanças do mercado – sejam elas de novas e evoluídas ameaças, sejam oriundas de novas regulações como a LGPD. Isso pode implicar em perda de competitividade e, em última análise, perdas financeiras.

Convencer as empresas de que educar seus times técnicos e colaboradores se traduz em benefícios concretos para os negócios é o principal desafio de um provedor de soluções e serviços como a Kaspersky. Para avançar, portanto, a companhia terá que ajudar seus clientes a montar a equação que permita comprovar os benefícios dessas iniciativas, traduzindo a mitigação de riscos de não-conformidade com leis e normas em valor para os negócios.

V. Conclusão

Diante de todas as transformações trazidas pela crise da COVID-19, as empresas tiveram que mudar para acompanhar os novos hábitos de seus clientes e parceiros de negócio. Os canais digitais ganharam maior relevância e, com eles, os dados dos clientes que por ali trafegam. Lidar com esses dados pessoais sensíveis ganhou uma nova dimensão sob o prisma da LGPD, e as empresas estão se preparando para isso.

A IDC acredita que as empresas precisarão investir no treinamento e conscientização de seus colaboradores para que estes possam entender mais claramente os impactos da LGPD sobre essas organizações. Cerca de 57% das empresas reconhecem desafio de definir novos papéis e responsabilidades no contexto de segurança diante da nova lei.

É preciso mostrar como *education* e conscientização revertem em prol dos resultados de negócio.

A Kaspersky visa oferecer um programa abrangente de educação para auxiliar essas empresas e sedimentar o conhecimento necessário nos times. Ao superar os desafios de convencimento da relevância dessas iniciativas – que, de fato, são importantes para o amadurecimento das empresas – e mostrar como isso reverte em prol dos resultados de seus clientes, a Kaspersky estabelecerá uma relação de confiança que a colocará em posição de destaque como *trusted advisor*.

V. Conclusão

Luciano Ramos, Gerente de Pesquisa e Consultoria

Gerente de Pesquisa e Consultoria do IDC, desenvolve programas de infraestrutura, software e serviços de TI, cobrindo o mercado brasileiro. Os estudos conduzidos por sua equipe fornecem aos clientes da IDC informações detalhadas sobre o tamanho do mercado, análises competitivas e previsões de TI no país.

IDC Custom Solutions

O conteúdo deste documento foi adaptado de estudos da IDC publicados em www.idc.com**.**

IDC Brasil

Av. Eng. Luis Carlos Berrini, 1645 – 8o andar

Brooklin Novo, São Paulo, SP, Brasil

+55-11-5508-3400

Twitter: @IDCLatin

www.idclatin.com

www.idc.com