Contexto Tecnológico

Transformação digital dos negócios

Edgar D'Andrea
Sócio Líder de Cibersegurança e Privacidade PwC Brasil

Em um ano conturbado, as empresas no Brasil buscaram na tecnologia formas alternativas para alcançar eficiência operacional e de custos, para criar diferenciação em serviços e produtos e para personalizar a experiência dos clientes.

A onda de inovação dos negócios por meio da tecnologia digital impulsionou o aparecimento de milhares de *startups* e novos negócios que, além de terem uma proposta disruptiva, possuem estruturas de custo bem mais enxutas quando comparadas com as dos conglomerados tradicionais.

Isso só aumenta o senso de urgência em relação à aplicação de novas tecnologias em um mundo cada vez mais digital. Nesse contexto, a figura a seguir mostra as oito tecnologias que empresas, de todos os setores, devem considerar na jornada de transformação digital dos seus negócios.

- Internet das Coisas
- Realidade aumentada
- Realidade virtual
- *Blockchain*
- Inteligência artificial
- Impressão 3D
- Drones
- Robôs

Análises avançadas de dados e conhecimento

À medida que os modelos de negócios e as capacidades digitais introduzem mudanças na sociedade, fica claro que dados e análises avançadas terão um papel fundamental no direcionamento das empresas digitais. Hoje, muitas empresas ainda não têm os recursos de dados e análises que gerem conhecimento mercadológico para fornecer experiências aos clientes certos no momento certo e no contexto certo.

À medida que as empresas buscam novos fluxos de receita, os dados primários surgem como um dos ativos mais valiosos. A robótica – com apoio de inteligência artificial, combinando sensores *IoTs* e uso de drones – pode, por exemplo, ser fonte de dados primários para modelos preditivos de conversão de novos clientes, determinando a probabilidade de um interessado ser convertido em um cliente.

Cibersegurança

Empresas de todos os países e segmentos estão investindo fortemente no uso das oito tecnologias essenciais para a inovação digital. Em um mundo altamente interconectado, os ecossistemas digitais proporcionam agilidade, interação e compartilhamento de informações críticas com clientes, fornecedores e parceiros de negócio. À medida que aumentam as suas conexões e a sua exposição às novas tecnologias, as organizações ficam mais vulneráveis aos riscos relacionados à segurança cibernética e à proteção de dados.

Ataques cibernéticos com impactos operacionais, financeiros e reputacionais significativos são cada vez mais frequentes. Episódios relevantes de vazamento de informações pessoais ou corporativas crescem de forma assustadora em todo o mundo. Os sequestros de dados por meio de *ransomware*, com o propósito de negociar pagamentos de resgates, inclusive por meio de criptomoedas para a “liberação dos dados”, se tornaram uma realidade em todos os segmentos empresariais.

Nesse contexto, monitorar e avaliar as ameaças e as medidas de proteção e remediação a serem adotadas pela administração das empresas deve ser uma preocupação dos conselhos de administração.

Cibersegurança e o regulador

Governos, autoridades, reguladores, empresários, consumidores e a sociedade em geral estão cada vez mais atentos com os avanços e impactos das violações cibernéticas e da proteção de dados.

Com isso, é fundamental que as empresas tenham prontidão, disciplina e coerência na gestão dos riscos cibernéticos e seus efeitos operacionais, financeiros, legais, regulatórios e reputacionais, por meio de programas estruturados de segurança e proteção de dados que permeiem todos os elementos das linhas de defesa da organização.

Banco Central do Brasil – Resolução nº 4.658 de 26/04/2018 e Circular nº 3.909 de 16/08/2018

O Banco Central do Brasil (Bacen) publicou em 26 de abril de 2018 a Resolução nº4.658, 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.

Seguindo a tendência internacional e em face dos recentes incidentes cibernéticos, o Bacen estabeleceu o posicionamento do regulador e os critérios a serem cumpridos em segurança cibernética, permitindo que as instituições reguladas avancem de maneira estruturada em um mundo cada vez mais digital, melhorem a relação de confiança com o mercado e sejam efetivas na gestão de riscos, *compliance* e controles internos; enfim, na governança cibernética.

A Resolução nº4.658 aborda questões objetivas e subjetivas, portanto a sua interpretação exige visão analítica e discussões internas de entendimento do âmbito de sua aplicação. Tópicos relevantes como serviços em nuvem no exterior, prontidão e transparência em casos de incidentes de segurança cibernética, compartilhamento de informações, envolvimento do conselho de administração, controle de informações sensíveis, classificação de dados e responsabilização por vazamento de informações sensíveis, que eram objeto de permanente discussão no mercado, são tratados na resolução, permitindo às instituições direcionarem suas decisões estratégicas, táticas e operacionais a este respeito.

Na mesma linha, a Circular nº 3.909 do Bacen estabeleceu os mesmos direcionamentos para empresas reguladas de meios de pagamento.

SEC Public Company Cybersecurity Disclosures, de 21/02/2018

A *Securities and Exchange Commission* (SEC) aprovou por unanimidade uma declaração e orientação interpretativa para auxiliar empresas abertas na preparação de divulgações sobre riscos e incidentes de segurança cibernética.

A Legislação Geral de Proteção de Dados (LGPD)

Um marco importante ocorrido este ano no Brasil foi a aprovação da Lei Geral de Proteção de Dados (LGPD) – Lei 13.709, de 15 de agosto de 2018. A LGPD dispõe sobre o tratamento de dados pessoais (de funcionários, de terceiros, de clientes, de fornecedores etc.), inclusive nos meios digitais, por pessoa natural ou jurídica de direito público ou privado, independentemente do país de sua sede ou do país onde estejam localizados os dados, considerando que (i) a operação de tratamento ocorra no território nacional; (ii) a atividade de tratamento esteja relacionada a oferta ou fornecimento de bens ou serviços a indivíduos localizados no território nacional; e (iii) os dados pessoais tratados tenham sido coletados no território nacional. O prazo para a conformidade com a lei é 16/02/2020.

Com isso, o Brasil se junta a diversos países do mundo que já possuem legislação sobre o tema. Na União Europeia, por exemplo, entrou em vigor em 25 de maio deste ano a Lei de Proteção de Dados Pessoais da EU, denominada General Data Protection Regulation (GDPR), a qual serviu de base para o texto aprovado no Brasil.

A LGPD trará implicações à sociedade e às empresas privadas e públicas no Brasil, que, além de precisarem rever suas políticas de tratamento de dados pessoais, deverão rever seus sistemas, processos e – por que não – seus modelos de negócios baseados em *analytics* e monetização de dados.

A Comissão de Proteção dos Dados Pessoais do Ministério Público do DF e Territórios (MPDFT), por exemplo, tem sido atuante nos casos de vazamento de dados pessoais no Brasil, exigindo explicações das empresas e ajuizando ação civil pública por danos morais coletivos com atribuição de valores a título de indenização por falta de cuidados da administração para garantir a segurança dos dados pessoais.

Nesse contexto, é enorme o desafio para que os executivos das empresas exerçam seu papel a fim de garantir o tratamento eficaz dos riscos cibernéticos e da proteção de dados, assim como os conselheiros em supervisionar os esforços das empresas em relação a segurança cibernética e proteção da privacidade de dados.

Ataques cibernéticos
- Crime organizado, ativistas, governos (direcionados)
- *Ransomware* (distribuídos)

- Prontidão
- Disciplina & controles Internos e *compliance*
- Confiança e coerência

Modelos de negócios digitais
- Serviços e produtos digitais
- *Analytics &* Monetização
- Parcerias & Terceiros

Evento cibernético adverso
(Fraude & Vazamento de dados)

Impacto:
- Operacional
- Financeiro
- Reputacional

Proteção de dados pessoais
- Bases legais na coleta e tratamento dos dados
- Princípios de Privacidade
- Direitos do titular

- Programa de proteção de dados e privacidade
- Gestão de resposta a incidentes de segurança cibernética
- Gestão de crises