CIOs na crise de Covid-19

Respostas táticas à “nova normalidade”

Maio2020

O CIO enfrenta hoje o maior desafio de sua carreira

Aproximadamente **quatro em cada cinco (77%) líderes brasileiros** passaram por ao menos uma crise corporativa nos últimos cinco anos.

A constatação é da primeira Pesquisa Global sobre Crises da PwC, um estudo com **2.084 executivos** de organizações de **vários portes**, em **25 setores** e **43 países, incluindo o Brasil.**

A pesquisa revelou ainda que, entre as crises mais graves enfrentadas pelas empresas, chamam a atenção questões de liquidez e problemas relacionados a tecnologia, como falhas operacionais e crimes cibernéticos.

Considerando esse contexto, entendemos que a crise causada pela pandemia de Covid-19 exercerá pressão, na área de tecnologia da informação, **principalmente sobre os CIOs**, que estão lidando com picos de sobrecarga nas estruturas de aplicações e infraestrutura, após a migração maciça das empresas para o trabalho remoto.

Em nossa visão, o CIO enfrenta hoje o maior desafio de sua carreira, marcado em muitas empresas do Brasil pelo colapso da infraestrutura, ataques cibernéticos, de fraude, de *ransomware* ou de negação de serviço (DoS) ou mesmo sites que saem do ar por excesso de tráfego.

Os CIOs desempenham papel central no enfrentamento da crise, seja atuando na estratégia da empresa para manter as operações em funcionamento, cuidando dos colaboradores, participando da proposição de novas formas de atuar em momento de crise ou mantendo a plena operação dos serviços e da infraestrutura digitais da empresa**.**

Nossa experiência mostra que há dezenas de atividades concorrentes em tempos de crise. Na situação atual, é essencial dar atenção às atividades operacionais relacionadas aos desafios da Covid-19, como :

- **Liquidez;**
- **Tecnologia (falhas);**
- **Crimes cibernéticos.**

> **“A cada dia, coisas novas acontecem. Na minha área de telemedicina, a demanda cresceu 37 vezes em uma semana.”**
>
> *CIO de uma das maiores seguradoras do Brasil*

O CIO enfrenta hoje o maior desafio de sua carreira

Liquidez

Como a TI se conecta?

O CIO deve se preocupar em entender quais contratos podem ser repactuados dentro de sua operação. O objetivo é obter ganhos nos valores finais e em termos de escala (fazer mais com menos). Também vemos que a automação de processos robóticos (RPA, na sigla em inglês) pode ser uma saída rápida e barata para ajudar na busca de eficiência e eficácia, direcionando a força de trabalho para atividades mais intelectuais.

Problemas de tecnologia

Como ter a estabilidade necessária nesta crise?

Manter a infraestrutura e as aplicações existentes sempre foi uma das atividades mais importantes do CIO. Avalie os serviços de TI utilizados pela empresa para verificar se contribuem para os resultados desejados, de curto ou médio prazo. Livre-se de sistemas ineficientes ou atualize-os com baixo investimento inicial, reduzindo custos e direcionando-os aos processos mais necessários no momento.

A crise deixou claro que infraestruturas e aplicações monolíticas precisam ser analisadas tanto do ponto de vista da arquitetura como da capacidade de crescer exponencialmente (escalabilidade). Hoje, os serviços de mobilidade para a força de trabalho e as aplicações nativas na nuvem estão crescendo nas TIs do Brasil.

Crimes cibernéticos

Como lidar com o risco cibernético e o aumento dos ataques e crimes digitais?

Antes da pandemia, os riscos cibernéticos já preocupavam os executivos, mas agora, com a nova realidade imposta pela Covid-19 e o aumento dos ataques cibernéticos, essa preocupação fica ainda mais evidente.

As áreas de segurança cibernética devem trabalhar em conjunto com as equipes de arquitetura, infraestrutura, gestão de riscos e *compliance* para coordenar as atividades de prevenção e detecção de ameaças e de resposta a casos de fraudes, vazamento de informações ou ataques cibernéticos.

Incidentes de segurança e privacidade de dados nesse período podem se transformar em passivos relevantes no pós-Covid-19, com impactos financeiros, operacionais e reputacionais.

> Um varejista de moda brasileiro que não tinha *e-commerce* colocou uma plataforma no ar em dez dias para manter o faturamento da empresa. Para conectar a nova plataforma aos sistemas legados, a atuação do CIO foi decisiva. Segundo ele, "**todas as discussões sobre *e-commerce* foram superadas, pois essa era a única alternativa para manter a empresa funcionando**."

Roadmap do CIO para o momento atual e o futuro próximo

Mobilizar
Reação à crise

Fase I:
construção de alicerces

- Diagnóstico de *Business Resilience.*
- Trabalho remoto.
- Infraestrutura e conectividade.
- Segurança, proteção de dados e monitoramento contínuo dos riscos cibernéticos.
- Sistemas críticos e redundância.
- Ecossistema de provedores.
- Práticas remotas de Agile.
- Foco em projetos prioritários, postergando e cancelando iniciativas, se necessário.

Estabilizar
Respostas táticas à "nova normalidade"

Fase II:
mergulho na resposta tática

- Continuidade de negócios.
- Otimização de custos.
- Arquitetura e performance.
- Aceleração e gestão de *cloud.*
- Redesenho da função, capacidade e espaço físico de TI.
- Gestão continuada da segurança cibernética e das operações de tratamento de dados pessoais.
- Otimização do portfólio de projetos.

Traçar estratégias
Como emergir ainda mais forte

Fase III:
busca de oportunidades

- Idealização e estabelecimento de novos canais digitais para potencializar a relação com clientes e parceiros de negócio.
- Pensamento digital – canais, serviços e produtos para os clientes.
- Repriorização das iniciativas de portfólio dos projetos.
- Otimização da segurança cibernética e da proteção de dados por meio de contratação de *Cyber* como serviço e investimentos pontuais (Capex) tendo foco no negócio.

O papel do CIO em cada fase da crise

Fase I

Mobilizar

Reação à crise

CIOs e líderes de tecnologia têm um papel fundamental nesta crise: garantir a operação e a continuidade do negócio, mantendo os empregados produtivos e conectados e estabelecendo níveis adequados de segurança cibernética.

Fase II

Estabilizar

Respostas táticas à "nova normalidade"

Na segunda fase, que abordamos em mais detalhes nesta publicação, a pressão por redução de custos, automação e redesenho da força de trabalho ganhará destaque nas ações táticas para enfrentar os desafios do negócio.

Fase III

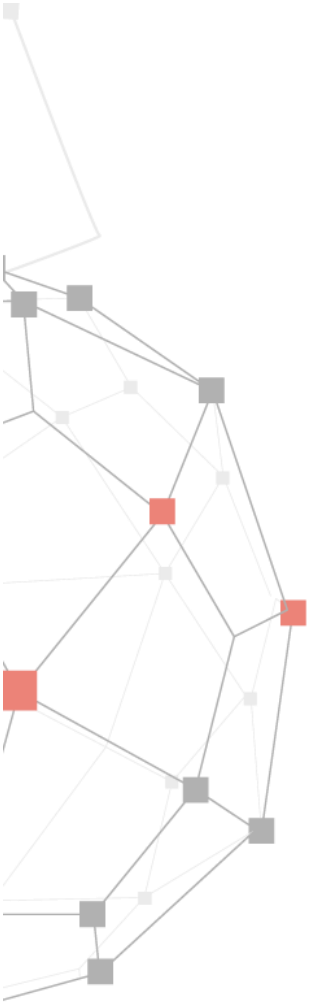
Traçar estratégias

Como emergir ainda mais forte

Nesta fase, os CIOs devem pensar na estratégia e em perspectivas para a "nova normalidade" pós-pandemia, direcionando a organização para o pensamento digital, apoiando a criação de canais digitais para clientes e parceiros de negócio e estabelecendo níveis de segurança cibernética e proteção de dados para permitir a verdadeira transformação digital da empresa.

Estabilizar

Respostas táticas à "nova normalidade"



Otimização de custos e portfólio

Fornecer resposta rápida às necessidades de otimização de custos no curto e médio prazo.

Avaliar a carteira com base no que poderá afetar o negócio e nas capacidades internas dos fornecedores.

Arquitetura e performance

Resolver rapidamente problemas de disponibilidade e performance dos sistemas e da conectividade.

Aceleração para *cloud*

Acelerar a migração de aplicações e componentes não críticos para *cloud*, otimizando performance e custos.

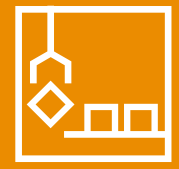
TI – novas formas de trabalho

Atenuar o impacto da interrupção dos sistemas, liberar capacidade de recursos humanos e otimizar o gerenciamento da força de trabalho de TI.

***Cybersecurity* e proteção de dados**

Rever a segurança de infraestrutura, dispositivos, apps e serviços digitais disponíveis local e remotamente.

Gerenciar de forma contínua os riscos cibernéticos, por meio de serviços de inteligência de ameaças, e operação de defesa cibernética, incluindo resposta a incidentes.



Automação – RPA

Aumentar a eficiência operacional e reduzir custos rapidamente, além de impulsionar a produtividade com a automação de tarefas. O trabalho remoto e a ausência de profissionais em licença pode ser um desafio, e o RPA pode ajudar.

Otimização de custos e portfólio

Principais desafios e preocupações

Em resposta imediata à crise, houve forte pressão para redução de custos.

Mas essas ações dificilmente são sustentáveis no médio prazo, se não houver um direcionamento para a otimização de custos. Certamente, as ações iniciais não leverão a organização a uma futura etapa de retomada.

A Covid-19 fez a sociedade se “acostumar com menos”, tanto pela percepção de que é possível entregar o essencial com menos recursos e investimentos quanto ao provocar uma reflexão sobre quais serão as reais necessidades futuras.

Ações

- Terceirização de serviços *commodities*: diante da pressão de custos, mesmo empresas mais conservadoras no tema perceberam os ganhos da otimização de serviços via parceiros especialistas em tarefas *commodities* de TI.
- Reavaliação de contratos: o momento sugere uma revisão dos parâmetros de fechamento de contratos vigentes, como: a curva de estimativa de demandas e o *baseline* das contratações; renegociação de taxas médias dos contratos antigos de renovação automática; consolidação de fornecedores; e fortalecimento de parcerias.
- Reavaliação de projetos: reavaliar os critérios de aprovação de projetos em andamento. Os retornos de investimentos poderão não se confirmar em um mercado retraído, a redução de pessoal pode já ter acontecido por força maior, as estratégias de expansão foram postergadas; cancelar ou postergar alguns projetos e focar e redirecionar outros projetos, buscando proteger o orçamento, agregar mais valor no novo cenário e antecipar retornos e *quick wins*.
- Atuação em relação a problemas crônicos: o resfriamento de novos projetos abre espaço para organizar a casa. Redirecione orçamento e talentos para iniciativas de manutenção corretiva e preventiva, a partir de uma análise de causas raízes que permita eliminar gastos de curto prazo usualmente dispensados em soluções de contorno.
- Indicadores de custos: se não existem, defina, implemente e monitore. Eles serão a base para as decisões.
- Sistemas ERPs: é importante revisar a priorização de demandas. Faça uma análise 80/20 dos maiores ofensores que impactam TI e Negócio (para isso, é possível usar ferramentas de gestão de incidentes) e crie *sprints* para atacar as maiores causas de problemas. Automações que têm um ciclo maior de desenvolvimento no ambiente ERP podem ser implantadas via RPA.
- Retomada: é hora de investir em projetos estruturantes que solucionem obsolescências graves, na ampliação do autosserviço com experiência otimizada (para clientes e empregados) para gerar eficiência, e em mobilidade e outras inovações essenciais, aproveitando que a pandemia ajudou a vencer algumas resistências. Aproxime-se de seus pares no negócio e de especialistas do mercado que o ajudarão a montar novos *business cases*.

Arquitetura e performance

Principais desafios e preocupações

Preocupações sobre a performance e a disponibilidade das aplicações críticas de negócio deverão ser prioridade na agenda de CIOs e gestores de aplicações e devem ser resolvidas rapidamente.

Por outro lado, as organizações que sofrem com a complexidade e a proliferação de tecnologias estão gastando uma proporção crescente de seus orçamentos de TI com manutenção e infraestrutura. O CIO precisa adotar medidas emergenciais para conter essa proliferação, além de avaliar possíveis *quick wins* em seu parque tecnológico.

Ações

- Analisar a jornada dos usuários para identificar os principais pontos de performance nos sistemas, na conectividade e em componentes tecnológicos. Entenda quais são os principais gargalos na visão dos usuários finais. Essa etapa permitirá uma rápida avaliação sobre quais processos de negócios e seus respectivos sistemas apresentam possíveis problemas de performance. Identifique esses problemas e execute ações rápidas para otimizar esses gargalos, como *load balance*, otimização do carregamento de informações (imagens, *scripts*, chamadas externas, entre outros) nas páginas acessadas, redesenho de APIs complexas, utilização de cache e índices de dados.
- Avaliar de forma rápida e segura potenciais otimizações de arquitetura nas aplicações. Também considerar nessa análise a transferência de *workloads* para *clouds* públicas com objetivos de otimização de custos de armazenamento.
- Estabelecer como prioridade do time de arquitetura a otimização de aplicações e componentes tecnológicos para reduzir custos de manutenção e reinvestir o valor economizado em outras necessidades do momento. Para isso, é necessário adotar uma abordagem em 3 etapas:

  1. Avaliar o parque tecnológico atual, incluindo aplicações e componentes tecnológicos.
  2. Avaliar a saúde desses componentes em relação ao negócio e à tecnologia, usando uma lente de TCO por aplicação e componente tecnológico.
  3. Otimizar as aplicações e componentes tecnológicos segundo 4 pilares (componente tecnológico defasado com alto valor para o negócio, componente obsoleto e sem valor ou com baixo valor, componentes maduros com pouco valor para o negócio e componentes maduros com alto valor).

Aceleração para *cloud*

Principais desafios e preocupações

Infraestruturas tradicionais não permitem crescimento na velocidade que a crise demanda. Aumentar a capacidade de processamento, memória e *throughput* será desafiador.

Conectar toda a força de trabalho remotamente demandará aumento de performance do ambiente de redes desde *firewall* até os links contratados.

Permitir acesso remoto a aplicações da empresa traz outro desafio para aplicações legadas e monolíticas que não permitem acesso facilitado via web. Transformar essas aplicações e acelerar a jornada para a nuvem é algo premente neste momento.

Ações

- A crise apresenta também oportunidades de negociação e avaliação de contratos empresariais com o provedor de *cloud*, com incentivos que podem reduzir os custos operacionais e de migração.
- Desligue recursos em horas não produtivas e use instâncias *Spot* e máquinas reservadas caso seu ambiente tenha previsão de funcionamento por longos períodos.
- Use no ambiente *cloud* uma política de *tag* para todos os recursos, a fim de identificar a aplicação ou área de negócio atendida. Isso ajudará a organizar seu ambiente e facilitará o processo de *billing*.
- Para a camada de redes e *firewall*, estenda as políticas internas da organização para os provedores de *cloud*, simplificando e acelerando o acesso a novas funcionalidades e mantendo o ambiente seguro com o uso de recursos como rede privada (Virtual Private Cloud) e Firewall de Aplicação (Web Application Firewall).
- Privilegie a contratação de serviços como PaaS ou SaaS. Isso dará velocidade e segurança para a migração do ambiente, tendo em vista que se trata de um período de resposta a crise. Configurar o ambiente do zero utilizando IaaS poderá acarretar maior tempo de migração e custos.
- Avalie as características de armazenamento de suas aplicações. Caso seja possível, utilize uma estratégia de *archiving* em *cloud*. Isso permitirá esvaziar uma área nobre de armazenamento e usar ofertas de baixo custo de *cold storage* em *cloud*.
- Avalie alternativas na cloud para demandas atuais no ambiente ERP. Extensões que alavancam APIs nativas do ERP em plataformas cloud (como SAP SCP, Azure e AWS) têm ciclo de implantação mais curto, menor TCO e garantem portabilidade para futuras atualizações do ERP.
- Avalie a possibilidade de migrar as aplicações que utilizam padrões como três camadas para *cloud*, facilitando e escalando o acesso remoto.

TI – novas formas de trabalho

Principais desafios e preocupações

Os impactos da Covid-19 nos diferentes segmentos de negócio desdobram os desafios da crise para as áreas de TI.

Além dos aspectos tecnológicos, questões relacionadas à organização das equipes e ao modelo de operação de TI também devem ser reavaliadas.

A tendência de digitalização de serviços e a movimentação de equipes para o ambiente remoto colocam em xeque a capacidade de entregar resultados relevantes para as áreas de negócio, que demandam mais e esperam agilidade maior.

Ações

- Preparar as equipes de suporte de TI para que possam atuar pra resolver um número maior de solicitações dos usuários. Em algumas indústrias, como varejo, educação e saúde, sistemas estão sobrecarregados, com potencial aumento de falhas e dúvidas de usuários e clientes. Também é necessário alinhar expectativas com as áreas de negócios e, se necessário, renegociar prazos de atendimento em razão do aumento das solicitações.
- Experimentar modelos que fortaleçam a colaboração e a agilidade na entrega e na tomada de decisão (em contraponto a modelos demasiadamente hierarquizados). A colaboração já é um elemento essencial, mesmo nas equipes que atuam de forma presencial. Esses modelos reforçam uma visão mais matricial da estrutura organizacional e do modelo de operação de TI. Na visão da PwC, as áreas de TI devem se organizar em estruturas virtuais de entrega de soluções e serviços e serem formadas por grupos multidisciplinares que reúnam as competências técnicas necessárias (visão *competence stack*).
- Adotar plataformas de colaboração para que as equipes de tecnologia possam atuar de forma remota e continuar contribuindo para que as entregas sejam atendidas com qualidade e dentro dos prazos e custos previstos. Há diversas opções de mercado que fornecem funcionalidades como conectividade de vídeo e áudio, colaboração na elaboração de documentos e compartilhamento e armazenamento de informações, entre outras.
- Automatizar o máximo possível a esteira de entrega de TI, diminuindo a intervenção humana e passagens de bastão desnecessárias, fortalecendo a integridade e a segurança das informações, e assegurando a gestão de conhecimento – seja ele técnico ou de negócio.

Cybersecurity e proteção de dados

Principais desafios e preocupações

O acesso a sistemas e recursos digitais da empresa passou a ser feito remotamente e por meio de dispositivos, pessoais ou corporativos, existentes na casa do colaborador, do terceiro ou do funcionário do prestador de serviços.

As práticas e controles de segurança da informação estabelecidos para colaboradores ou exigidos para os parceiros de negócio (AMS, *Call Centers* etc.) podem ter perdido sua eficácia e aplicabilidade.

Os ataques e golpes cibernéticos se intensificam, explorando a desatenção das pessoas e as vulnerabilidades de dispositivos, serviços e apps digitais.

Ações

- A primeira linha de defesa é fundamental para as organizações e envolve boas práticas de segurança nas operações da empresa que devem estar refletidas em processos, tecnologia e pessoas. A execução das funções corporativas em casa – pelo colaborador ou pelo terceiro – exige o mesmo rigor em termos de segurança da informação que no ambiente corporativo. Mensagens educativas aos colaboradores e revisão das exigências contratuais de práticas de segurança de terceiros são inciativas importantes.
- O acesso remoto deve ser objeto de controle e monitoramento sistemático por parte das empresas, a fim de prevenir ou identificar prontamente casos de ataques cibernéticos resultantes de fragilidades em computadores e dispositivos remotos ligados à rede da empresa. Ferramentas que conferem maior segurança ao acesso privilegiado e/ou remoto são fundamentais.
- O gerenciamento contínuo dos riscos cibernéticos, por meio de serviços de inteligência de ameaças e de defesa cibernética, incluindo resposta a incidentes, é ainda mais importante para as empresas neste momento.
- Os responsáveis por segurança cibernética devem atuar em conjunto com as equipes de gestão de riscos e prevenção a fraudes para coordenar as atividades de prevenção, detecção de ameaças e de resposta a casos de fraudes ou incidentes cibernéticos.
- As empresas devem estar atentas à segurança das operações de tratamento de dados pessoais, considerando o contexto da Lei Geral de Proteção de Dados (LGPD). Qualquer vazamento de dados pessoais neste momento poderá se tornar um passivo legal e regulatório no futuro próximo.
- Ações de segurança de perímetro, por meio de tecnologias de proteção de borda, são fundamentais, garantindo a disponibilidade e integridade dos serviços e a proteção dos dados corporativos.
- O uso de autenticação de dois fatores (2FA ou MFA) para acesso aos recursos corporativos é mandatório neste momento.

Automação – RPA

Principais desafios e preocupações

Nos tempos atuais, rápidas mudanças e adaptações podem acelerar a transformação digital. A busca por redução de custos e maior eficiência operacional é uma preocupação neste momento.

Altos volumes de pedidos no *e-commerce* (e todo o impacto disso no *back office*), processamento de alto volume de dados no governo, necessidade de eficiência e agilidade no processamento de testes médicos, aumento de ligações em *call centers*, empresas buscando dados para cuidar de seus empregados e alta demanda para renegociação de dívidas nos bancos. O RPA pode ser de grande utilidade para atender a essas necessidades.

Ações

- Identifique atividades repetitivas realizadas por humanos e que registraram queda de produtividade por causa do isolamento social ou da licença de profissionais infectados pelo vírus.
- Alguns segmentos apresentaram um aumento significativo nos volumes de processamento, como varejo on-line, *call centers* e bancos. O RPA pode ajudar a reduzir ou eliminar o *backlog* e aumentar a eficiência das operações durante a crise. Hospitais e laboratórios no mundo adotaram a automação de processos, por exemplo, para vencer a sobrecarga de sistemas e de atendimento.
- A automação de processos de *back office* pode ser implementada rapidamente. No entanto, também há ganhos muito significativos na automação de processos no *mid* e *front office*. Nesses casos, uma combinação de soluções com o RPA (*chat bot*, inteligência artificial, *machine learning*, *data & analytics*) trará ganhos sustentáveis e importantes de médio e longo prazo.
- Iniciativas com potencial redução de custos podem ser uma saída para garantir a continuidade dos negócios no curto e no médio prazos. A automação de processos melhora o custo operacional, reduz ou otimiza custos com *headcount* e diminui perdas ocasionadas pela não realização de atividades e/ou por *backlog* represado pela falta de mão de obra.
- Procure fazer um *scale up* dos negócios com o uso de robôs. O ROI da implementação da iniciativa de RPA é facilmente medido e pode ser alcançado em um tempo curto.
- O RPA pode ser usado para ERPs em duas situações:
  - ERP em uso pela empresa – é possível aplicar a solução para processos rotineiros e maduros;
  - Implantação de ERP – pode ser muito bem aplicado durante a fase de testes tanto para validação dos processos como para testes de volume, aproveitando a força de trabalho para análise dos resultados, em vez da execução de tarefas.

Contatos

Para mais informações, entre em contato com a nossa equipe:

Andrea França

Sócia
andrea.França@pwc.com

Norberto Tomasini

Sócio
norberto.t.tomasini@pwc.com

Eduardo Ebel

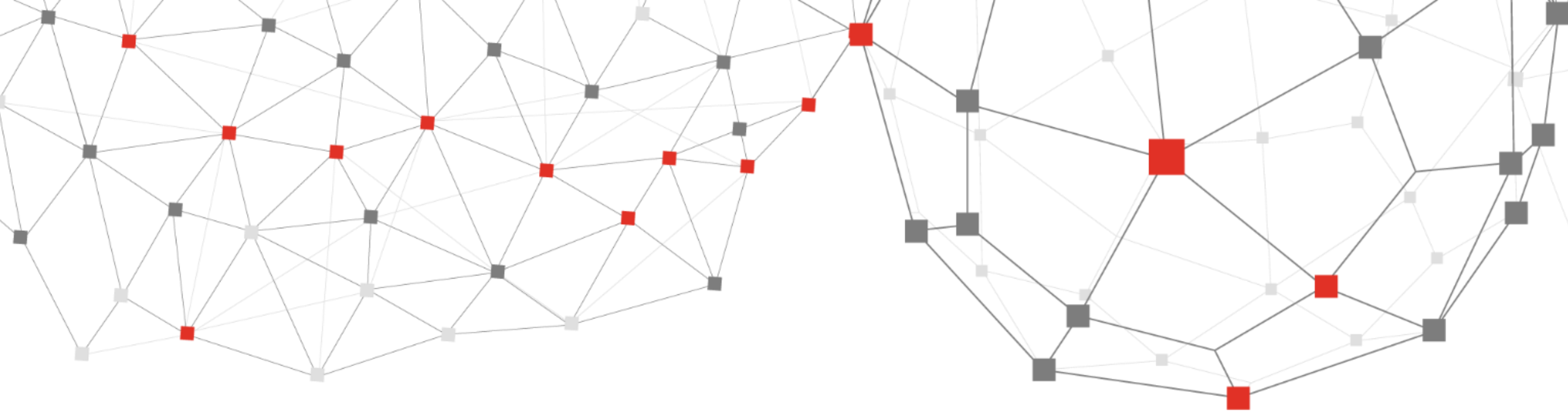
Sócio
eduardo.ebel@pwc.com

Fernando Mitre

Sócio
fernando.mitre@pwc.com

Felipe Almeida

Diretor
felipe.almeida@pwc.com



PwC. Traga desafios. Leve confiança.
www.pwc.com.br

PwC Brasil @PwCBrasil @PwCBrasil PwC Brasil PwC Bras

Neste documento, “PwC” refere-se à PricewaterhouseCoopers Tecnologia da Informação LTDA, firma membro do network da PricewaterhouseCoopers, ou conforme o contexto sugerir, ao próprio network. Cada firma membro da rede PwC constitui uma pessoa jurídica separada e independente. Para mais detalhes acerca do network PwC, acesse: www.pwc.com/structure