IDC ANALYZE THE FUTURE

IDC VENDOR SPOTLIGHT

Patrocinado por: Oracle

Nunca foi tão evidente a necessidade de ter os negócios preparados para enfrentar cenários adversos, sejam eles causados por erros humanos, desastres naturais ou, até mesmo, uma pandemia como a da COVID-19.

Estratégia de Continuidade de Negócios e Como Construir um Plano de Recuperação de Desastres

Maio, 2021

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

I. Introdução

Nunca uma crise impactou as economias globalmente como a pandemia da COVID-19. Diante desse cenário, as empresas tiveram que reaprender e reinventar as maneiras de colaborar e fazer negócios – o que implicou em estar mais disponível e suportar mais clientes nas plataformas e canais digitais. Soma-se a isso a necessidade de atender às novas regulamentações e desafios impostos pelas iniciativas globais para combater a mudança climática. Consequentemente, as organizações tiveram que buscar maneiras mais eficientes, muitas vezes incluindo tecnologia da informação, para controlar crises econômicas e ambientais.

Essas são lições que as sociedades e os países não podem ignorar. A resiliência se tornou uma prioridade. No entanto, as abordagens tradicionais lutam para integrar seus planos de continuidade de negócios com o novo ambiente digital no qual as empresas devem operar. A IDC sugere que CEOs, CFOs e outros executivos *C-Level* trabalhem lado a lado com os CIOs para adicionar tecnologia para apoiar a organização durante esta crise e qualquer outra no futuro.

EM DESTAQUE

IMPORTÂNCIA DA NUVEM

69% das empresas pretendem alcançar uma estratégia ideal de migração de cargas de trabalho para nuvem nos próximos 12 meses.

TENHA EM MENTE

A escolha do *data center* para DR deve considerar as necessidades de continuidade dos negócios das organizações, juntamente com as peculiaridades do território brasileiro, incluindo topologia, hidrografia, baixa incidência de tremores, entre muitas outras.

Os executivos podem usar *frameworks* específicos para identificar os pontos fracos da resiliência digital e priorizar iniciativas de tecnologia direcionadas, casos de uso, bem como mudanças de processos/políticas que aumentam a resiliência em diferentes funções e em toda a empresa.

Sem dúvida, a Recuperação de Desastres (*Disaster Recovery* ou DR em inglês) é parte essencial das estratégias de continuidade de negócios e tem sido uma tendência em empresas que passaram a se posicionar com papel preponderante a partir da pandemia da COVID-19. IDC vê esses mercados com crescimento robusto nos próximos anos; por exemplo, em 2020, os gastos globais de DR como serviço foram de cerca de US$ 4,9 bilhões.

Atualmente, as empresas enfrentam uma infinidade de desafios como:

- Ameaças cibernéticas, como ataques de *ransomware*, crimes cibernéticos e outros riscos à segurança.
- Erros humanos e desastres sociais, como a pandemia da COVID-19, guerras ou quedas econômicas.
- Desastres ambientais, como inundações, secas, incêndios, terremotos e furacões, entre muitos outros.

Nesse contexto, as empresas devem ter estratégias, planos e soluções tecnológicas para prevenção e recuperação de desastres como componentes essenciais de sua continuidade de negócios. Essas medidas as ajudam a evitar perdas financeiras e problemas organizacionais para manter um ambiente de trabalho saudável para os funcionários, a dinâmica da cadeia de valor e, por fim, a relação com seus clientes.

Muitas organizações consideram o planejamento de recuperação de desastres uma tarefa complexa e pouco familiar. Os desastres acontecem tão raramente que as operações de recuperação não fazem parte da rotina. Além do mais, a miríade de dados, aplicativos e outros recursos interconectados que teoricamente seriam recuperados após um desastre tornariam a recuperação um esforço desafiador e sujeito a erros. Mas então, no início de 2020, a pandemia da COVID-19 atingiu o mundo todo; desde então, organizações e governos, não apenas no Brasil, mas em todo o planeta, têm aprendido o significado de transformação digital acelerada, recuperação de desastres e continuidade de negócios da maneira mais difícil.

Mesmo aquelas companhias que normalmente prestavam pouca atenção à recuperação de desastres agora estão aprendendo que todo plano de continuidade de negócios e DR precisa abranger como os sistemas e dados estarão disponíveis com todas as atividades necessárias para manter a operação dos negócios. Por exemplo, questões como as relacionadas à logística da cadeia de suprimentos são cruciais quando ocorre um desastre; a TI desempenha um papel fundamental em manter os sistemas e dados disponíveis para que os processos continuem a fluir.

Nesse sentido, a construção de um plano para recuperação de desastres e continuidade de negócios à luz dos requisitos obrigatórios tem duas partes principais:

- Implementar a TI, entrelaçando infraestrutura e cargas de trabalho, para proteger todos os dados e garantir a disponibilidade, bem como os processos operacionais e transacionais.
- Manter o cumprimento das normas de forma clara e expressa, gerar relatórios e documentar todos os procedimentos a serem elaborados em caso de auditoria; os auditores precisam ver se os planos de DR e continuidade de negócios existem e protegem adequadamente os ativos de dados corporativos.

O ponto crítico é que nenhum elemento pode ser ignorado; recursos físicos, de TI e humanos não podem agir isoladamente uns dos outros.

II. Definição e Propósito de DR

Hoje, qualquer sistema confiável voltado para organizações ou o público deve ser construído para esperar o inesperado. Nenhum sistema é perfeito e, em algum momento, algo imprevisto pode acontecer e afetar o negócio: pode ser um incêndio, um furacão, uma enchente, um terremoto, um erro humano, entre muitos outros eventos. Como os sistemas

podem falhar de tantas maneiras possíveis, eles devem ser projetados com uma mentalidade de prevenção de falhas e desastres.

Existem dois tópicos relacionados definidos abaixo que são frequentemente misturados, mas essenciais na arquitetura de sistemas para ajudar a prevenir e mitigar falhas: Alta Disponibilidade (HA, ou *High Availability* em inglês) e Recuperação de Desastres (DR).

Alta Disponibilidade (HA)

A alta disponibilidade elimina pontos únicos de falha e mantém todos os dados disponíveis para os usuários; isso implica em redundância. Ao longo do histórico de HA, a redundância tem sido uma necessidade na maioria dos sistemas:

- A **redundância de *hardware*** marcou a introdução da alta disponibilidade na computação. Os aplicativos se interconectaram em redes para atender às necessidades dos negócios.
- A **redundância de *software*** veio em seguida. Os desenvolvedores de aplicativos garantiram que os sistemas poderiam tolerar falhas devido ao *hardware*, configuração ou qualquer outro motivo externo que causasse mal funcionamento do software.

Atualmente, a redundância de *hardware* ocorre em *racks* de servidores dentro de *data centers* (sejam eles próprios ou terceirizados, *on-premises* ou na nuvem), incluindo rede, energia e armazenamento com *hardware* que permite aos usuários distribuir cargas de trabalho e mitigar pontos únicos de falha. A redundância do *data center* em uma região geográfica, comumente conhecida como "zona de disponibilidade", permite que os usuários executem aplicativos a partir de *data centers* separados geograficamente, mas próximos uns dos outros.

Todos esses domínios (*hardware*, *software* e ambiente) procuram resolver o mesmo problema fundamental que é eliminar pontos únicos de falha. Os resultados fornecem um alto nível de acordos de serviço (SLA, ou *Service Level Agreement* em inglês) que medem o tempo de inatividade não planejado e o mantém nos menores patamares possíveis durante um determinado período de 24 horas.

Recuperação de Desastres (DR)

A recuperação de desastre é o processo de colocar um sistema de volta em seu estado operacional quando ele fica inoperante. Em essência, DR entra onde a alta disponibilidade falha – portanto, HA vem primeiro – e pode ser tão simples quanto restaurar de um *backup* ou se tornar extremamente complexo; tudo depende de dois fatores:

- ***Recovery Time Objective* (RTO):** É a quantidade máxima de tempo que um sistema pode ficar inativo antes de ser recuperado para seu status operacional. Às vezes, o RTO pode ser medido em horas ou até dias.
- ***Recovery Point Objective* (RPO):** É a quantidade de perda de dados tolerável em um desastre medida no tempo. Alguns sistemas podem considerar a perda de um dia de dados aceitável, enquanto outros não podem tolerar a perda de minutos ou mesmo segundos de dados.

O fato é que a criticidade das cargas de trabalho determina a duração do RTO e do RPO e pode ter consequências profundas e implicações graves para a empresa sobre como os planos de recuperação de desastres são implementados.

RTO e RPO curtos exigem que os sistemas implementem a replicação de dados ativa entre o sistema primário e os sistemas de recuperação em um estado para estarem prontos para assumir o controle no caso de um desastre. Da mesma forma, o gatilho para recuperação de desastres deve ser sempre automatizado e inteligente. Por exemplo, cargas de trabalho altamente críticas estariam idealmente disponíveis em dois domínios na mesma região e interconectadas com uma rede criptografada de baixa latência. Isso é especialmente importante quando falamos de sistemas que rodam em um ambiente *on-premises*.

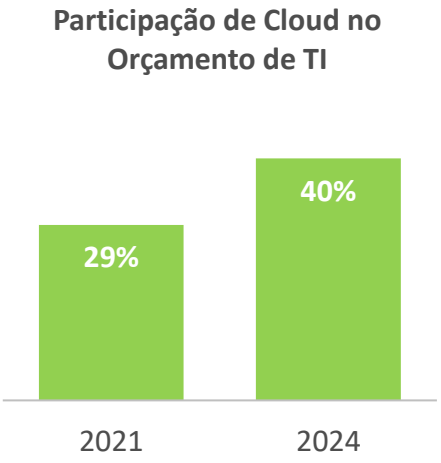
Fundamentalmente, HA e DR visam o mesmo objetivo: manter os sistemas ativos e funcionando em um estado operacional, seja no local ou na nuvem – com a principal diferença sendo que o HA pretende lidar com os problemas enquanto os sistemas estão em execução; já o DR trata dos problemas depois que os sistemas falham. Independentemente de quão altamente disponível um sistema possa ser, qualquer carga de trabalho, não importa o quão trivial seja, precisa ter um plano de recuperação de desastres em vigor.

Recuperação de Desastres, Computação em Nuvem e Maturidade das Empresas

Falando sobre a infraestrutura ideal para estar pronto para recuperação de desastres e alta disponibilidade, as arquiteturas de nuvem oferecem alto desempenho e resiliência. Uma arquitetura equilibrada entre físico e virtual aumenta a segurança e o desempenho; além disso, permite o consumo sob demanda de serviços em nuvem, como bancos de dados em *cluster* e recursos inteligentes de segurança.

Nesse contexto, os clientes podem distribuir seus aplicativos em diferentes domínios de falha, permitindo proteção contra falhas comuns de *hardware* ou energia e mantendo seus dados protegidos em caso de um desastre, como inundações, terremotos ou furacões, ao mesmo tempo em que oferece suporte à manutenção contínua; isso fornece resiliência e redundância extras.

FIGURA 1: ***Cloud x Orçamento de TI no Brasil***



Fonte: IDC LA Public Cloud Services Tracker, 2020H2 / IDC LA Private Cloud Tracker, 2020H2

Quando se trata de selecionar *data centers* e serviços em nuvem, as empresas estão amadurecendo. De acordo com o estudo *IDC Latin America IT Investment Trends 2020*, 69% das empresas pretendem alcançar uma estratégia ideal de migração de cargas de trabalho.

No entanto, o Brasil continua a ser uma região com extensos legados de TI, conectividade e aplicações de negócios.

A IDC estima que os serviços de computação em nuvem representam, em média, cerca de 29% do orçamento anual voltado para a infraestrutura de TI para empresas brasileiras em 2021, com perspectiva de chegar a 40% até 2024. Isso mostra que as organizações continuarão a se concentrar na nuvem.

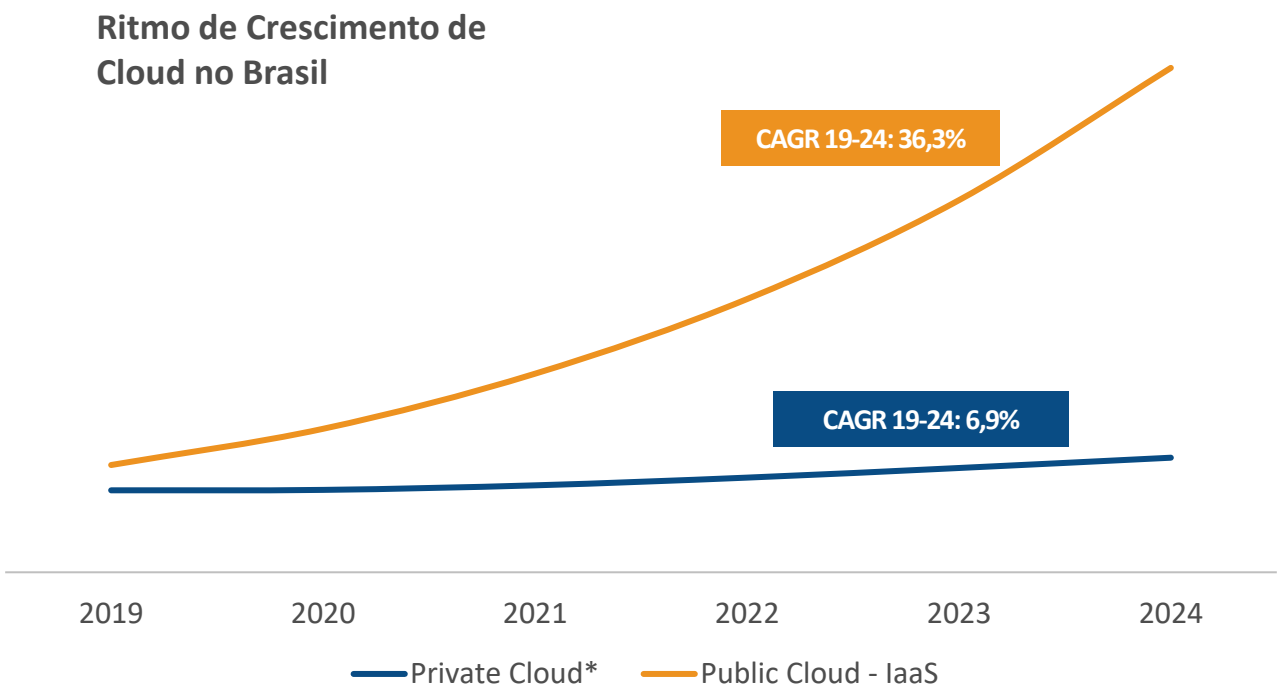
Os serviços Infraestrutura como Serviço (IaaS) em nuvem pública terão taxa de crescimento anual composto (CAGR em inglês) de 36,3% de 2019 a 2024. Além disso, haverá um CAGR de 6,9% no mesmo período para projetos de nuvem

privada. Esses investimentos estão associados a estratégias que abordam cargas de trabalho transacionais e críticas, bem como uma quantidade significativa de inovação aproveitando tecnologias como a Internet das Coisas (IoT), Inteligência Artificial (IA) e *Machine Learning* (ML).

A IDC vê os ambientes híbridos como a primeira escolha para empresas latino-americanas entre 2021 e 2024, devido à grande quantidade de *data centers* e infraestrutura de servidores, armazenamento e conectividade *on-premises* ainda prevalecentes, e também porque as empresas que fizeram pesados investimentos anteriores em soluções locais decidiram adotar modalidades *as a service* enquanto continuam a se beneficiar de infraestruturas existentes. No Brasil, 83% das empresas ainda têm cargas de trabalho locais em *data centers* próprios, mas a metade dessas empresas já usa algum tipo de nuvem junto com esses recursos.

Em 2023, as empresas brasileiras esperam ter aproximadamente 50% de suas cargas de trabalho em execução na nuvem. A IDC vê que a recuperação de desastres e a alta disponibilidade são estratégias essenciais para garantir a continuidade dos negócios e alcançar maior agilidade.

FIGURA 2: ***Expectativa para o Mercado de Cloud no Brasil***



Fonte: IDC LA Public Cloud Services Tracker, 2020H2 / IDC LA Private Cloud Tracker, 2020H2

Desastres do Mundo Real que as Organizações Podem Prevenir

Os desastres podem acontecer a qualquer momento; as empresas estão sujeitas a riscos ambientais, crimes, acidentes e crises de saúde, como a pandemia da COVID-19, que levou as organizações a estarem mais conscientes da necessidade de flexibilizar a infraestrutura e desenvolver planos de DR.

Embora muitos perigos possam ser de natureza cíclica, eles nem sempre desencadeiam uma resposta importante das organizações que buscam manter sua continuidade de negócios. Eventos como terremotos, furacões e inundações repentinas acontecem, mas geralmente são vistos como raros. No entanto, uma rápida olhada no relatório do OCHA (Escritório das Nações Unidas para a Coordenação de Assuntos Humanitários) relativo a 2000-2019, publicado em março de 2020, mostra o contrário. Na verdade, a América Latina é a segunda região mais propensa a desastres em todo o mundo. Talvez ninguém possa evitar desastres naturais, mas as empresas podem controlar a perda de dados associada.

TABELA 1: ***Desastres Naturais no Brasil em Números***

	Impactos
Inundações	O Brasil está classificado entre os 15 principais países globalmente com a maior população exposta ao risco de enchentes de rios. Em 12 ocasiões desde 2000, as inundações no Brasil e na América Latina causaram mais de US$ 1 bilhão em danos totais.
Tremores	Cerca de 25% dos terremotos de magnitude 8,0 ou superior ocorreram na América do Sul. Ainda que, em sua maioria, aconteçam distantes dos grandes centros, seus impactos podem abalar vastas regiões e comprometer serviços de infraestrutura.
Secas e Incêndios	Mais de 33 milhões de pessoas são afetadas pelas secas no Brasil. Esse fenômeno somado a fortes ventos e altas temperaturas, comumente causa incêndios florestais com potencial de causar grandes danos à infraestrutura crítica ou às comunidades.

Fonte: ONU

Quanto aos riscos de segurança cibernética, conforme a pandemia da COVID-19 progredia durante o primeiro trimestre de 2020 e as empresas adotaram casos de uso como *home office* e aprendizagem remota, quase três milhões de ataques cibernéticos ocorreram na região. Em março de 2020, o número de vírus de computador aumentou 131% em comparação com março de 2019, pois o tráfego da *web* aumentou na maioria das áreas urbanas.

Em setembro de 2020, quase 56% dos ataques cibernéticos na América Latina tinham como alvo usuários ou infraestruturas no Brasil, enquanto aproximadamente 28% tinham como alvo usuários no México e 10% na Colômbia.

Em 2020, Brasil e Venezuela foram os dois países com a maior incidência de ataques de *phishing*, com 19,94% e 16,84%, 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%. (Fonte: Statista)

Até a chegada da COVID-19, as empresas experimentaram o impacto coletivo de grandes perturbações juntamente com choques climáticos recorrentes. Todas essas dificuldades juntas estão levando as companhias a criarem planos de recuperação de desastres complexos e multidimensionais. A pandemia acelerou a transformação digital e gerou a necessidade de adaptação a mudanças repentinas que exigiam que os funcionários enfrentassem novas necessidades de negócios e tecnologias para cobrir *home office*, *e-commerce*, mobilidade, digitalização e automação de procedimentos, para citar apenas alguns. As empresas reavaliaram suas prioridades em relação aos casos de uso que precisaram ser digitalizados ou criaram novos para atender às necessidades repentinas desde o início da pandemia. O *home office*, por exemplo, tornou-se um padrão essencial, apesar de ter levado mais de um ano para que a companhias criassem políticas

para regular sua aplicação e proteger os dados considerando novos ambientes de conectividade e potenciais riscos envolvidos.

Os exemplos a seguir mostram situações que envolvem a restauração de dados em um cenário de DR, comuns no Brasil e no mundo.

Destruição do Data Center: Sem dúvida, um dos piores cenários que uma empresa moderna pode enfrentar é um desastre natural como um furacão, uma enchente ou um terremoto que destrói uma seção ou todo o *data center*. Embora essas situações pareçam raras, basta lembrar do último terremoto na Cidade do México em 2017, furacões afetando os estados do sul dos EUA, chuvas fortes, deslizamentos de terra, inundações e incêndios florestais no Brasil em 2020. Nesses casos, a destruição ambiental somada a surtos elétricos pode causar perda permanente de dados.

A melhor maneira de preparar as organizações para a recuperação é garantir que haja cópias externas de todos os dados. Se as informações estiverem *on-premises*, já é hora de pensar em manter *backups* na nuvem em que os dados possam ser facilmente armazenados e acessados com segurança. As organizações precisam ter uma maneira de garantir a continuidade dos negócios, mesmo que suas instalações principais tenham sido afetadas; um plano de DR adequado incluiria também alternativas como *home office* e até mesmo realocação de emergência de alguns funcionários.

De forma geral, é preciso medir os riscos e estar preparado para manter o negócio funcionando, independentemente da localização. Esta indicação também se aplica ao *data center*; é importante ter um *data center* fora da área de risco, mas perto o suficiente, e fornecer redundância na nuvem para garantir que as organizações possam reduzir o tempo de inatividade – ou até mesmo zero *downtime*.

Ataques de Segurança Cibernética (DDoS): Em um ataque de negação de serviço distribuído (DDoS), a rede fica sobrecarregada com solicitações ilegítimas e os dados não podem ser transmitidos. Como resultado, a organização não pode mais conectar seus recursos de TI (como aplicações e bancos de dados, por exemplo), o que gera ruptura.

Nesse cenário, DR significa ser capaz de restaurar a disponibilidade dos dados mesmo quando o ataque DDoS está em andamento. Neste ponto, as empresas devem ter uma cópia de seus dados seguros em outra estrutura, seja num *data center* ou na nuvem. No entanto, o que é crucial em ter uma infraestrutura alternativa é a capacidade de disponibilizar esse *backup* para produção colocando novos servidores *online* para hospedá-lo. Mais uma vez, *data centers* estrategicamente próximos tornam-se parte dos planos de DR em termos de redundância, RTO e RPO mais curtos possíveis.

Sabotagem de Dados: Um terceiro exemplo de desastre visto na maioria das regiões e países em todo o mundo acontece quando alguém – como um funcionário insatisfeito – sabota dados deliberadamente ou permite acesso a outros atores mais perversos e perigosos, como cibercriminosos. O desastre pode ir desde a inserção de informações imprecisas, código malicioso ou bugs em sistemas até um ataque DDoS ou *ransomware* que imobiliza a organização e gera altos custos inesperados. Além de um trabalho constante de conscientização, é crítico na prevenção desse tipo de desastre garantir que as organizações tenham ambientes de recuperação atualizados e prontos.

Existem muitos outros tipos de riscos e eventos que podem afetar a continuidade dos negócios, como greves, roubos, acidentes de trabalho, falhas de energia, erros humanos e atividades e ameaças geopolíticas, etc. Por qualquer motivo, os riscos estão sempre presentes e a melhor maneira de lidar com eles é com um plano de HA e DR adequado ao perfil, atividades e localização da organização.

III. Benefícios de uma Estratégia de Recuperação de Desastres

Em geral, o principal benefício de ter uma estratégia adequada de DR é a continuidade dos negócios. Ao prevenir desastres de todos os tipos e ter alta disponibilidade de informações, é possível atingir os objetivos de negócios rapidamente:

- Planejar com visão de futuro.
- Manter os objetivos de receita e redução de custos, apesar das mudanças e possíveis interrupções.
- Adaptar-se às mudanças nos mercados e às demandas dos clientes.
- Ganhar a confiança dos clientes e de toda cadeia de valor.
- Atingir metas de lucratividade e produtividade de negócios.

Em suma, a aplicação adequada de técnicas de recuperação de desastres ajudará qualquer organização a ser produtiva, inovadora e adaptável a qualquer mudança em seu ambiente.

IV. Contexto Atual

Em 2020, as empresas lutaram para se adaptar e investiram em projetos que abordassem suas fraquezas resultantes da pandemia. A recuperação e os investimentos continuarão para algumas organizações à medida em que surgem novos requisitos operacionais. O ano de 2021 está abrindo novos capítulos com transformação digital e resiliência no topo de suas prioridades.

A ênfase desses novos temas organizacionais – e os investimentos novos/incrementais associados, principalmente dedicados à modernização da infraestrutura – dependerá da maturidade da nova mentalidade da empresa, das respostas contínuas à crise do COVID-19 e de situações que se desenhem em paralelo a metas de negócios e organizacionais mais amplas.

A economia da América Latina começou 2021 com uma perspectiva positiva; o Fundo Monetário Internacional (FMI) prevê um aumento de 4,6% em dólares constantes para 2021. No entanto, o crescimento econômico da região parece lento e depende da rapidez com que os países implementem planos de vacinação para conter a COVID-19 e alcançar uma reativação econômica sustentada. A previsão de crescimento para 2021 no Brasil, México, Chile, Colômbia e Peru foi revisada para cima, e os auxílios emergenciais estimularam a ativação econômica e ajudaram muitas famílias a sobreviver em face do desemprego.

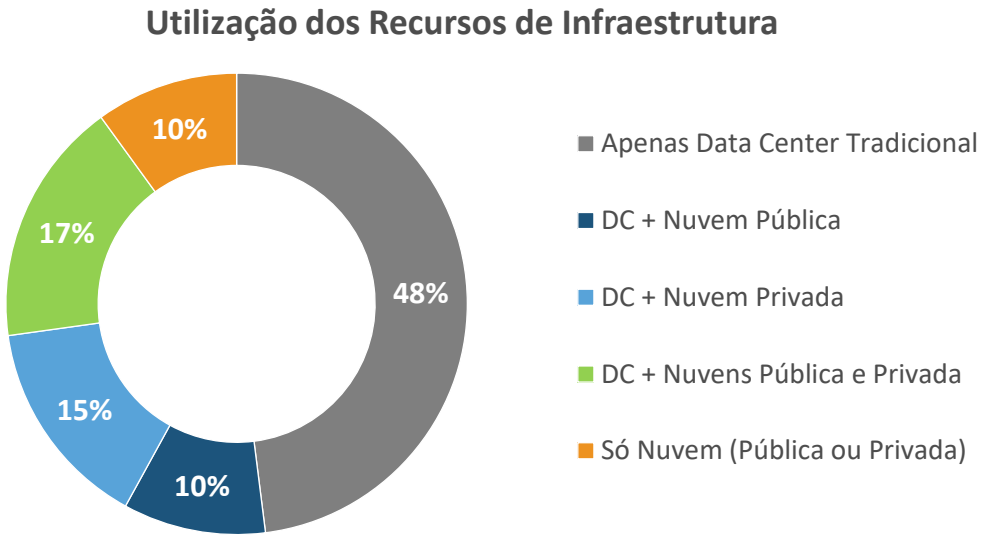
O principal interesse das empresas é transformar os atuais serviços ao consumidor para criar novas experiências multicanais em B2C e B2B, como em novas plataformas para gerenciamento de ativos, comércio eletrônico, mídia social, transações bancárias e métodos de pagamento.

Em 2021, 69% das empresas latino-americanas com mais de 500 funcionários que avaliam serviços em nuvem se concentram em:

- Definir as cargas de trabalho mais viáveis e as prioridades em uma estratégia de migração para uma plataforma de computação em nuvem.
- Familiarizar-se com a migração para melhor avaliar as implicações técnicas, comerciais, funcionais e econômicas da nuvem.

A IDC acredita que a primeira escolha e padrão no Brasil entre 2021 e 2024 serão os ambientes híbridos, enquanto o ritmo de progresso em direção à nuvem pública e privada continuará a acelerar. As estratégias de infraestrutura já estão focadas na nuvem. De acordo com o *IDC Brazil Hybrid Cloud Study 2020*, 51% das empresas de grande porte já usam mais de um provedor de nuvem pública para IaaS e PaaS, enquanto 48% das empresas usam atualmente algum tipo de nuvem privada. A distribuição dos recursos de infraestrutura das organizações pode ser vista na figura a seguir.

FIGURA 3: ***Infraestrutura de TI no Brasil***



Fonte: IDC Brazil Hybrid Cloud Study, Novembro 2020

Atualmente, 33% das grandes empresas brasileiras já estão integrando diferentes ambientes de nuvem de vários provedores em uma abordagem de nuvem híbrida; outros 17% o farão nos próximos 12 meses. Sua estratégia é direcionada principalmente para:

- Modernização e mobilidade de aplicativos.
- Integração de dados em nuvem.
- Gerenciamento de infraestrutura e orquestração.

Nesse cenário, as empresas brasileiras estão reavaliando suas prioridades quanto à digitalização de casos de uso ou à criação de novos para atender às novas demandas do mercado. O *home office*, por exemplo, tornou-se um padrão, assim como os pagamentos eletrônicos, o comércio eletrônico e os serviços de saúde digitais, portanto, já há

investimentos nessa direção. Essas organizações já estão gerando experiências digitais por meio de componentes de realidade virtual, usam sensores em cadeias de suprimentos com elementos de IoT e usam inteligência artificial em serviços de emergência essenciais. Todos esses serviços digitais significam uma operação 24 horas por dia, 7 dias por semana, necessitando de colaboração contínua. Suas cargas de trabalho críticas precisam de RTO e RPO muito curtos para atender aos requisitos de transparência, segurança, eficiência e facilidade de uso necessários para agregar valor e ganhar a confiança de clientes e gerar mais receitas.

V. Tendências de Recuperação de Desastres

Diante dos novos contextos e da aceleração da transformação digital trazida por eles, as organizações se concentraram na resiliência e na capacidade de habilitar novas tecnologias. A IDC vê dois grandes grupos de investimentos que endereçam essas necessidades:

- **Investimento no núcleo digital:** Compreende gastos de TI nos principais componentes da resiliência digital – TI centrada na nuvem, segurança, suporte para o trabalho remoto e projetos de transformação; isso deve aumentar com o tempo, na medida em que o orçamento de TI vai deixando os gastos tradicionais e legados.
- **Investimento em inovação digital:** Inclui o investimento em TI atual e previsto com foco em novas tecnologias adicionadas ou reposicionadas que atenderão aos novos requerimentos de negócio.

Embora a inovação seja um grande *drive* para investimentos em novas tecnologias, as empresas precisam evoluir continuamente seu núcleo digital para acompanhar as tendências de mercado. Somando-se a essa necessidade o fato de que os riscos de desastres precisam ser mitigados, vamos que não é à toa que DR ganham impulso em resposta a esses desafios.

Olhando para o futuro, a IDC vê as seguintes tendências de DR em 2021 e nos anos seguintes:

Multicloud

As organizações latino-americanas percebem que não estão limitadas em relação à nuvem. Uma estratégia *multicloud* fornece um caminho fácil para a redundância de dados e ambientes. Além disso, as empresas ficam livres para escolher seus provedores, permitindo avaliar continuamente serviços e preços. Outros benefícios, como certificações e conformidade, podem oferecem uma vantagem maior na preparação e capacitação de times.

Recuperação de Desastres como Serviço - DRaaS

A recuperação de desastres como serviço replica os serviços físicos ou virtuais de uma empresa para fornecer *failover* durante uma crise. O *Disaster Recovery as a Service* (DRaaS) elimina a carga do DR interno e garante RTOs e RPOs mais curtos para organizações com cargas de trabalho de missão crítica na nuvem, bem como outros SLAs de que possam precisar. A tendência emergente de digitalização, juntamente com a crescente adoção de serviços baseados em nuvem em todos os setores, é um dos principais fatores que impulsionam o crescimento do DRaaS. Tais soluções eliminam a necessidade de um local de recuperação secundário e oferecem recuperação de dados mais rápida e menos complexa e maior visibilidade de *backup* em nuvem, além de vários avanços tecnológicos, como a introdução de replicação inteligente de dados, inventário de máquinas virtuais, testes automatizados com IA e ML, e a possibilidade de automação da proteção de ambientes virtuais, que se mostra eficiente diante do crescimento de ataques cibernéticos.

Automação Inteligente

A automação dos processos de *backup* e de recuperação já são itens comuns e continuarão sendo. No entanto, a partir de 2020, a tendência adiciona elementos de IA e ML para priorizar os dados durante esses processos, ou para excluir dados com base em critérios de relevância e segurança para mantê-los protegidos, detectando e interrompendo automaticamente comportamentos maliciosos.

A tecnologia continuará a avançar e as redes das organizações continuarão a evoluir e se expandir em funcionalidade e geografia. As empresas continuarão a se adaptar a forças de trabalho remotas, muitas delas a longo prazo, se não permanentes, sendo que parte dessa força recorrerá a dispositivos móveis. As empresas exigirão novas estratégias de DR para manter seus dados seguros e acessíveis.

Por volta de 2024 e além, as organizações continuarão planejando com foco na resiliência. Seus investimentos de núcleo digital incluirão os cuidados para garantir que elas reestabelecerão suas operações no menor tempo possível se ocorrer um desastre. Dado o grande número de infraestrutura *on-premises* ainda prevalecente, a IDC acredita que, até 2023, a modalidade de nuvem híbrida se tornará uma prioridade para 90% das organizações latino-americanas com mais de 500 funcionários; no Brasil, 51% das grandes empresas já estão movendo suas cargas de trabalho críticas para a nuvem, enquanto 54% estão priorizando a modernização e mobilidade de aplicativos, de acordo com o estudo *IDC Brazil Hybrid Cloud Study 2020*.

VI. Perfil do Fornecedor

A Oracle é uma empresa global com escritórios, *data centers* e parceiros nos cinco continentes. A Oracle busca usar a Tecnologia da Informação (TI) para fornecer vantagens competitivas aos clientes, reduzir seus custos operacionais, melhorar sua comunicação com os clientes e aumentar as percepções de gerenciamento de seus negócios.

A Oracle vê que as empresas estão cada vez mais dependentes de sua infraestrutura de TI, e os eventos recentes aceleraram seu interesse em novas tecnologias e resiliência. Portanto, precisam de disponibilidade contínua. A Oracle criou a *Oracle Maximum Availability Architecture* (MAA), que visa fornecer um conjunto de planos de melhores práticas para o uso integrado de suas tecnologias para recuperação de desastres (*Disaster Recovery* ou DR) e alta disponibilidade (*High Availability* ou HA) e garantir níveis ideais de disponibilidade.

A Oracle aporta mais de 30 anos de experiência na solução dos problemas de HA mais desafiadores por meio de soluções para reduzir o *downtime* para interrupções planejadas e não planejadas para clientes com as cargas de trabalho mais exigentes e requisitos para ambiente *on-premises*, em nuvem ou em nuvem híbrida.

Empresas com qualquer tipo de infraestrutura podem contar com a Oracle para fornecer soluções de DR e HA com tecnologia de software Oracle, que inclui RMAN, *Data Guard* e *Active Data Guard*, *Golden Gate* e RAC para Exadata e ZDLRA (HW).

Ao longo das décadas, o Oracle MAA evoluiu em várias direções para fornecer as melhores práticas e recomendações de projetos como parte de uma implementação integrada e projetada que é encontrada em seus *Engineered Systems*, como o *Oracle Exadata Database Machine*, já disponível na Oracle Cloud. O *Oracle Database Cloud Services*, um serviço de PaaS (*Platform as a Service*, ou plataforma como serviço) na Oracle Cloud, tem como objetivo operar seguindo os

padrões que garantem a máxima disponibilidade para os clientes Oracle. E o *Oracle Autonomous Database* oferece a máxima automação para segurança e disponibilidade para bancos de dados rodando na nuvem.

A Oracle visa atuar como um *advisor* para qualquer gestor de TI que deseja atingir o mais alto nível de disponibilidade, porque seus projetos consideram e discutem os vários cenários de falha que podem afetar um ambiente crítico. No que se refere aos bancos de dados Oracle, a empresa pretende dar um passo além e tem como objetivo fornecer uma solução baseada nos recursos integrados de HA da Oracle.

A *Oracle Cloud Infrastructure* (OCI) tem o objetivo de fornecer vários blocos de construção para planejar a abordagem de DR:

- **Regiões:** Cada região da OCI está em uma área geográfica independente e separada, às vezes por grandes distâncias; são instalações distribuídas entre regiões, países e continentes.
- **Domínios de Disponibilidade:** Refere-se a um ou mais *data centers* localizados em uma região. Eles são isolados um do outro, são tolerantes a falhas e dificilmente falharão simultaneamente.
- **Domínios de Falha:** Um grupo de *hardware* e infraestrutura dentro de um domínio de disponibilidade; cada um deles contém três domínios de falha. Os domínios de falha permitem que as organizações distribuam seus recursos para maior proteção.

A Oracle busca manter um objetivo de nível de serviço de *uptime* de 99,95% (um máximo de 22 minutos de tempo de inatividade por mês), e com as práticas recomendadas pela Oracle MAA para serviço contínuo as empresas podem ter a maioria dos meses efetivamente com tempo de inatividade zero. Muitos desses objetivos de nível de serviço estão em contrato padrão, com penalidades caso a Oracle não alcance tais objetivos.

A Oracle pretende fornecer vantagens na nuvem ao disponibilizar mais regiões para suportar a recuperação de desastres real para seus clientes incluindo a nova região de Vinhedo, no interior paulista, para ser a opção de DR em nuvem para a região de São Paulo. A escolha do local da nova região permite garantir uma latência muito baixa com a de São Paulo, para atender requisitos de DR e de alta disponibilidade. Embora o tráfego de comunicação entre as regiões possa ser cobrado, a Oracle pretende fornecer uma abordagem de preço que permita o controle preciso dos custos de conectividade.

Desafios

Um dos maiores desafios que impedem as organizações de implementar alta disponibilidade e RTOs e RPOs curtos é o custo. Quando se trata de HA, mais redundância requer mais recursos, o que se traduz em custos mais elevados. De maneira geral, os principais desafios enfrentados pela Oracle neste quesito são:

- Custo e complexidade para implementação da estratégia.
- Falta de profissionais capacitados para implementar tal estratégia.
- Risco de falha no planejamento dos objetivos de recuperação.

Sobre este último item, peguemos um exemplo. Para a maioria das empresas que usam *backup* em fita, o RPO é de 24 horas (geralmente fazem um *backup* todas as noites), então o RTO pode demorar até 48 horas antes que todos os dados sejam recuperados e os aplicativos voltem a funcionar. O custo dessa estratégia, em termos de perdas, pode ser inaceitável nos ambientes digitais atuais.

Por outro lado, RTOs e RPOs curtos exigem a capacidade de lidar com *failover*, o que também se traduz em custos mais altos. A solução é sempre ter uma infraestrutura ideal na nuvem e equilibrar a prioridade e criticidade das cargas de trabalho e ter domínios de disponibilidade dentro da região interconectados por uma rede criptografada de baixa latência.

A IDC aconselha as empresas a terem planos robustos de continuidade de negócios para garantir que as operações possam ser retomadas o mais rápido possível ou, melhor ainda, continuar sem interrupções. Toda empresa deve se planejar para o pior, mas isso não quer dizer que seja fácil. Abaixo estão alguns outros desafios a serem superados:

- Alinhar a recuperação de desastres com os imperativos de negócios.
- Aproveitar redundâncias para minimizar interrupções.
- Cumprir as obrigações de segurança e conformidade da indústria.
- Manter o plano de DR executado à risca.

VI. Conclusões e Recomendações

À medida que a transformação acelera, as empresas continuarão a levar sua infraestrutura para a nuvem. No entanto, o Brasil ainda possui uma grande parcela de infraestrutura *on-premises*, o que traz a nuvem híbrida como prioridade. Diante dessa situação, os serviços de DR na nuvem são a preferência e a tendência. Além disso, as organizações devem considerar o comportamento dos desastres naturais no país.

É essencial ter *data centers* próximos e interconectados como parte de uma estratégia de redundância e resiliência.

A IDC recomenda que a escolha do *data center* para localização de DR considere as necessidades de continuidade dos negócios das organizações, juntamente com as peculiaridades do território brasileiro, incluindo topologia, hidrografia, baixa incidência de tremores, entre muitas outras.

Assim, é fundamental avaliar:

- Distância entre as instalações: deve ser razoável, sendo perto o suficiente para assegurar benefícios de conectividade, mas fora de uma área geográfica que possa ser afetada por um mesmo desastre.
- Fornecimento de serviços redundantes de infraestrutura para os *data centers*, como energia e telecomunicações.
- Condições geológicas, como falhas e bacias hidrográficas, para certificar que os *data centers* evitam rotas de inundação.

- Rotas de aviação, para garantir que as instalações não sejam cruzadas pelas mesmas rotas e, eventualmente, afetadas por desastres com aeronaves.
- Instalações como campos de mineração e represas nas proximidades, para que as rotas de emergência não afetem os *data centers*.

É essencial ter *data centers* próximos e interconectados como parte de uma estratégia de redundância e resiliência contra qualquer tipo de desastre natural, cibernético e até humano. Essa infraestrutura resiliente e dinâmica permitirá que as empresas tenham RTO e RPO mais curtos, especialmente devido à necessidade de muitas delas que operam 24x7 e colaboram continuamente em tempo real.

Plano de Continuidade de Negócios

Olhando para o futuro, a IDC considera que as empresas devem se concentrar em planos de continuidade de negócios com base em uma infraestrutura digital que tire proveito de uma arquitetura aberta, integrada e holística. Esta estrutura de resiliência digital inclui três fases que descrevem o cronograma de respostas diante de uma crise:

1. Responder e restaurar: Nesta fase, as organizações devem se concentrar nas atividades de recuperação, enfatizando a proteção da força de trabalho, a recuperação de desastres dos sistemas e a preservação do dinheiro. Certifique-se de que as tecnologias digitais críticas que dão suporte durante este estágio se concentrem no plano de continuidade, no gerenciamento de crises e na comunicação. Este não é o momento para análises profundas, planejamento ou investimento; este é o momento de agir rápido.

2. Expandir e otimizar: Uma vez recuperadas de um desastre e funcionando, as organizações nesta fase devem se concentrar nas atividades de estabilização; enfatizar a produtividade; acelerar a tomada de decisão; manter-se ao alcance do cliente; estabilizar cadeias de suprimentos e controlar de custos. Uma vez que as ameaças estejam para trás, a empresa pode analisar, planejar e investir com cautela. Seria hora de melhorar, expandir e otimizar as capacidades tecnológicas para operar como um negócio digital em um ambiente de crise. Os investimentos digitais típicos nesta fase são modestos e envolvem relatórios e inteligência aprimorados, migração para nuvem, trabalho remoto, privacidade e segurança, dados e otimização da cadeia de suprimentos.

3. Acelerar e inovar: As organizações nesta fase estão operando amplamente focadas em atividades de transformação. Crises novas e diferentes surgirão inevitavelmente, então este seria o momento de incorporar a resiliência digital como um princípio básico, prepara-se para o futuro e avançar. Os investimentos digitais nesta fase são maiores e focados em arquiteturas dinâmicas, modelos cognitivos, análises em tempo real, gêmeos digitais, desenvolvimento nativo da nuvem, gerenciamento de reputação e gerenciamento de conhecimento.

Plano de Recuperação de Desastres

Dentro de cada plano de continuidade de negócios, todas as empresas – pequenas e grandes – devem ter um plano de recuperação de desastres em sua resposta e fase de restauração. A IDC sugere que todas as organizações realizem uma análise de risco e impacto nos negócios pelo menos uma vez por ano e a tornem dinâmica para evitar riscos repentinos e sem precedentes, como a pandemia da COVID-19.

As empresas devem sempre ter em mente que um plano de recuperação de desastres visa:

- Criar estratégias e procedimentos para ajudar uma organização a retomar as operações normais após um desastre.
- Alcançar níveis de produção normais ou quase normais no menor tempo possível.

A análise do impacto de um desastre determina as funções de negócios mais críticas na organização e os ativos e cargas de trabalho necessários.

Ao analisar esses pontos, é possível saber o impacto e a perda para então planejar com antecedência. Sobretudo, considere que a resposta adequada a esses riscos minimiza o efeito do desastre. Por exemplo, no caso de um desastre natural, uma grande manufatura pode ter a capacidade de enviar seus funcionários para trabalhar em casa e mover algumas operações para uma fábrica próxima.

Talvez uma linha de produtos tenha que ficar fora do mercado, mas os sistemas têm que estar em pleno funcionamento, para que as outras áreas possam continuar operando e outros produtos continuem no mercado. A operação não para; é apenas uma área que foi danificada.

Para chegar lá, responder a perguntas como as que elencamos a seguir pode ajudar a obter as informações necessárias para tomar decisões importantes sobre a recuperação de desastres.

- Quais dados são necessários para manter a continuidade dos negócios?
- Quais são os sistemas prioritários e cargas de trabalho por área?
- Qual é o RTO e RPO mínimos por área?
- Quais são as funções de negócios críticas e não críticas por área e como elas funcionam?
- Qual é a perda de receita por hora, por área e por produto em caso de paralisação da produção?
- Qual é o requisito mínimo de pessoal para manter o negócio operacional?
- Quais são os ativos mínimos necessários?

O que se segue seria uma organização que aprende e que cria novos ecossistemas, inova e alavanca as operações de negócios ágeis. O redesenho e a reinvenção dos modelos de negócios se tornariam uma prioridade e, claro, o planejamento para estar pronto para a próxima crise e além.

Sobre o Analista

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