Quanto custa montar um e-commerce no Brasil?

O comércio eletrônico brasileiro deve ultrapassar R$ 220 bilhões em faturamento este ano, segundo dados do setor. Mas além do crescimento, chama atenção outro número: montar um e-commerce competitivo para empresas em 2025 pode custar entre R$ 170 mil e R$ 500 mil, dependendo do modelo de negócio e do nível de maturidade digital

A estimativa é da Backlgrs, startup especializada na implementação de Salesforce no Brasil, que acaba de divulgar uma análise sobre os investimentos médios necessários para empresas que desejam lançar ou transformar sua presença online, tanto no B2C quanto no B2B. A análise da empresa também reforça que e-commerces dentro dessa faixa de investimento já contam com alta disponibilidade (99,99%), infraestrutura robusta e histórico comprovado de estabilidade — sem falhas mesmo em datas críticas como a Black Friday.

relif_CANVA

"A diferença entre um e-commerce que cresce de forma sustentável e outro que estagna ou quebra está na capacidade de estruturar um ecossistema tecnológico verdadeiramente seguro, personalizado, escalável, integrado e centrado no cliente — seja ele final ou corporativo. Em 2025, o improviso já não tem mais espaço. O consumidor está mais exigente, o mercado mais competitivo, e as margens mais apertadas. Quem ainda trata o digital como canal secundário está perdendo relevância. Investir em tecnologia não é mais uma vantagem — é uma condição básica de sobrevivência no mercado atual.", afirma Guilherme Carvalho, CEO da Backlgrs.

- Investimentos variam conforme o modelo e a complexidade da operação - De acordo com o levantamento, para operações B2C, o custo inicial pode variar de R$ 50 mil a R$ 300 mil, considerando o porte da empresa, a personalização da experiência do usuário e a integração com sistemas como ERP, CRM e logística. No entanto, esse intervalo costuma abranger plataformas iniciais, que podem não oferecer o nível ideal de personalização, segurança e disponibilidade exigido por operações mais robustas.

Já no modelo B2B — que exige um nível ainda maior de customização e gestão de relacionamento — o investimento pode superar R$ 500 mil, dependendo da complexidade da operação. Tanto no B2C quanto no B2B, os projetos considerados referência já incorporam recursos de alta disponibilidade, personalização profunda da experiência e mecanismos que garantem performance estável mesmo em picos de acesso.

Segundo Carvalho, um dos grandes erros das empresas ao iniciar no digital é subestimar a complexidade da jornada de compra online. "No B2B, por exemplo, a automação de processos, a personalização por cliente, e a integração com sistemas legados são essenciais. No B2C, a experiência precisa ser fluida, omnichannel e com suporte em tempo real. Tudo isso tem custo mas também alto retorno quando bem executado."

- **Tendência é de soluções modulares e escaláveis** - A Backlgrs destaca ainda a tendência crescente do uso de plataformas modulares, como o Salesforce Commerce Cloud, que permitem que empresas iniciem com uma base sólida e escalem conforme o crescimento do negócio. Isso reduz riscos, garante mais estabilidade e facilita a adaptação às mudanças do mercado — sem comprometer a performance da operação.

"Hoje, vender online é apenas o ponto de partida. O verdadeiro diferencial está na capacidade de criar jornadas digitais consistentes, personalizadas e contínuas. As empresas que entendem isso estão construindo relacionamentos duradouros com seus clientes, baseados em confiança e valor percebido. Para isso, não basta estar presente no digital é preciso investir de forma inteligente em tecnologia, dados e estratégia para entregar experiências relevantes em escala," conclui Carvalho. - Fonte e mais informações: (https://www.backlgrs.com.br/).

Burnout entre lideranças

Sob pressão constante por performance e tomada de decisão, lideranças estão entre os grupos mais afetados pelo burnout.

O cansaço das lideranças tem nome: burnout. A síndrome, antes associada majoritariamente a profissionais da linha de frente, hoje encontra nas lideranças um dos grupos mais afetados. Dados de centros internacionais como a Nascia revelam que seis em cada 10 líderes já enfrentaram sintomas de esgotamento profissional. No Brasil, a preocupação se intensifica: o país bateu recorde de afastamentos por transtornos mentais em 2024, com mais de 470 mil licenças concedidas pelo INSS.

"É um problema estrutural. Estamos vendo gestores adoecendo por não conseguirem lidar com a pressão de resultados, a sobrecarga emocional e a responsabilidade sobre o clima organizacional. É urgente entender que cuidar da liderança é também cuidar do negócio", destaca Michel Cabral, CEO da Vixting, HR & Health Tech com 15 anos de atuação em saúde ocupacional.

A síndrome de burnout é caracterizada por exaustão física, emocional e mental, desmotivação, irritabilidade, isolamento e queda de desempenho. Nas lideranças, esses sintomas são muitas vezes camuflados pelo desejo de manter uma imagem de resiliência e controle, o que dificulta ainda mais a identificação precoce do problema.

A solidão de quem lidera

Além da sobrecarga funcional, líderes relatam uma solidão crônica. Muitos evitam expor suas vulnerabilidades por medo de parecerem fracos ou incompetentes, o que amplia o risco de adoecimento silencioso. "As empresas ainda esperam dos líderes um perfil inalcançável: resiliente, presente, motivador e incansável. Essa expectativa, muitas vezes desconectada da realidade, é uma das raízes do problema", comenta Cabral.

Como o RH pode atuar de forma estratégica

A Vixting reforça que o papel do RH precisa ir além das rotinas operacionais. O setor deve se posicionar como aliado estratégico na promoção da saúde emocional das lideranças, com ações como:

- Capacitação para o reconhecimento de sinais precoces, como mudança de comportamento, irritabilidade, excesso de controle ou retração;
- Estímulo à cultura de autocuidado e escuta ativa, com abertura para conversas seguras e livres de estigma;
- Flexibilização de jornadas e metas realistas, com acompanhamento frequente;
- Implementação de sistemas inteligentes, que integrem dados de saúde ocupacional e rastreiem padrões de risco, permitindo uma atuação preventiva e personalizada.

A tecnologia como aliada da prevenção

Com foco na digitalização dos processos de saúde ocupacional, a Vixting desenvolve soluções que apoiam o RH na construção de ambientes mais saudáveis. A plataforma permite que empresas monitorem atestados, identifiquem sinais de risco e criem trilhas de cuidado personalizadas para diferentes perfis de liderança.

"O RH do futuro precisa unir empatia, dados e agilidade. Só assim conseguiremos agir antes que o burnout destrua carreiras, comprometa equipes e impacte os resultados das empresas", finaliza Michel Cabral.

Resiliência Contra Ransomware: Um Guia de Ações Essenciais

Gustavo Leite (*)

A crescente sofisticação dos ataques de ransomware exige uma abordagem abrangente, que vai além das estratégias tradicionais de backup e recuperação

A resiliência cibernética, nesse contexto, deve ser construída a partir de uma combinação de preparação organizacional, práticas técnicas robustas e processos claros de resposta e recuperação.

Mais do que proteger dados: resiliência cibernética

Muitas organizações acreditam que a continuidade dos negócios e a recuperação de desastres são suficientes para enfrentar ameaças digitais. No entanto, a verdadeira resiliência exige a capacidade de restaurar não apenas sistemas de produção, mas também plataformas de autenticação, comunicação e segurança, que são essenciais para uma resposta eficaz a incidentes.

Ataques destrutivos, como os que apagam dados ou comprometem a infraestrutura, mudam o fluxo tradicional de resposta. Nesses casos, a restauração das capacidades de comunicação e resposta é tão importante quanto a recuperação dos dados em si.

Preparação: o papel das pessoas e dos processos

A preparação começa pela formação de uma equipe multidisciplinar, com responsabilidades bem definidas para cada etapa de resposta. É fundamental que todos saibam como agir caso os meios de comunicação principais estejam indisponíveis, quem lidera cada função e quais são os contatos alternativos. Simulações realistas de incidentes ajudam a identificar pontos fracos e alinhar expectativas.

Além disso, o risco de ransomware deve ser integrado à gestão de riscos corporativos. Isso garante que o tema receba a devida atenção estratégica e recursos adequados. Uma política clara sobre ransomware deve estabelecer critérios para declaração de incidentes, estratégias de backup e condições para tomada de decisões críticas, como pagamento de resgate.

Redução de riscos técnicos

Reduzir a superfície de ataque é essencial. Isso inclui limitar privilégios administrativos, aplicar autenticação multifator, segmentar redes e revisar periodicamente os acessos. O controle rigoroso do acesso remoto e o monitoramento constante dificultam a movimentação de invasores dentro do ambiente.

Os backups, por sua vez, precisam ser protegidos de forma rigorosa. Manter cópias isoladas e imutáveis, testar regularmente os processos de restauração e restringir o acesso administrativo aos sistemas de backup são práticas indispensáveis para garantir que a recuperação não reintroduza artefatos maliciosos.

Detecção e resposta ágeis

A capacidade de detectar rapidamente um ataque faz toda a diferença. Monitoramento em tempo real de logs e eventos, uso de ferramentas de correlação e caçadas proativas por sinais de comprometimento são práticas recomendadas. Testes regulares dos processos de detecção e resposta garantem que a equipe esteja preparada para agir sem hesitação.

No momento do incidente, a resposta deve ser coordenada: isolar sistemas afetados, preservar evidências para análise forense e iniciar a recuperação a partir de backups limpos. A comunicação deve ocorrer por canais alternativos, sempre com mensagens claras e alinhadas para todos os públicos envolvidos.

Recuperação e melhoria contínua

A restauração dos serviços deve priorizar os sistemas críticos, validando a integridade antes do retorno à produção. O monitoramento pós-recuperação é fundamental para detectar possíveis reinfecções. Após o incidente, reuniões de lições aprendidas permitem atualizar políticas, reforçar treinamentos e revisar planos, promovendo uma cultura de melhoria contínua.

A resiliência contra ransomware é um processo dinâmico, que depende da integração entre tecnologia, processos e pessoas. A preparação, a resposta rápida e a busca constante por aprimoramento são as bases para minimizar impactos e garantir a continuidade dos negócios diante de ameaças cada vez mais sofisticadas. Organizações que investem nessas práticas estão mais aptas a enfrentar e superar os desafios impostos pelo cenário atual de cibersegurança.

(*) Vice-presidente para América Latina da Cohesity.