PME: quando trocar o ERP básico por uma plataforma robusta?

Marco Vonzodas (*)

Grande parte das pequenas e médias empresas (PMEs) inicia sua trajetória com sistemas de gestão genéricos ou módulos básicos, que dão conta do recado nos primeiros passos. No entanto, conforme o faturamento avança e a operação ganha novas camadas de complexidade, como múltiplos canais de venda ou gestão de estoque mais exigente, a ferramenta que antes organizava a rotina passa a travar o negócio.

Segundo dados da FGV-CIA (Centro de Tecnologia de Informação Aplicada), cerca de 80% das médias empresas brasileiras já utilizam algum sistema integrado de gestão. No entanto, esse indicador cai para 35% e 40% entre micro e pequenas empresas, onde a gestão ainda depende de planilhas isoladas.

O sinal mais claro de alerta surge quando a empresa passa a trabalhar em volta do sistema, e não com ele. Na prática, isso aparece na proliferação de planilhas paralelas, no retrabalho de digitar o mesmo dado em vários lugares e nos fechamentos contábeis e fiscais lentos, dependentes de ajustes manuais e de uma única pessoa que "sabe como tudo funciona".

Soma-se a isso a dificuldade de integração com e-commerce, CRM, bancos e o fisco, além de customizações que travam atualizações legais e relatórios divergentes que fazem cada área obter um número diferente. Quando o gestor precisa perguntar "será que esse número está certo?" antes de tomar uma decisão, o ERP já deixou de ser um aliado.

Esse cenário é reforçado pela edição de 2026 da Pesquisa de Maturidade Digital dos Pequenos Negócios, do Sebrae em parceria com a ABDI (Agência Brasileira de Desenvolvimento Industrial), que registrou a média de 39 pontos em uma escala de 0 a 80. O estudo revelou que 60% das PMEs se enquadra na categoria de "Emergentes", que representa o segundo estágio de digitalização, reunindo negócios que já saíram do nível analógico ou iniciante, mas ainda não integraram a tecnologia de forma estratégica à sua gestão.

Manter um sistema defasado dá a falsa sensação de economia, mas consome recursos silenciosamente. Para enxergar o peso desse "barato que sai caro", o caminho é transformar o incômodo operacional em reais por mês, dividindo a conta em quatro blocos: produtividade perdida da equipe (horas de retrabalho multiplicadas pelo custo/hora com encargos), histórico de erros fiscais e operacionais dos últimos 12 meses, margem das vendas perdidas por ruptura ou atrasos e o custo da decisão tardia, que gera compras erradas e estoque parado.

Ao somar esses fatores em base anual — incluindo os gastos atuais com licenças, infraestrutura e consultores acionados para remendar falhas — e comparar com o investimento em uma plataforma robusta, o diagnóstico costuma ser revelador. Muitas vezes, a empresa já paga o preço de um sistema novo em ineficiência, mas sem receber nenhum dos benefícios.

Não existe um número mágico de faturamento que determine a hora exata da troca, pois o que dita esse movimento são os gatilhos de complexidade. A convivência de mais de uma operação fiscal (indústria, comércio e serviço juntos), logística com múltiplos armazéns e controle de lotes, alto volume de transações, exigência por governança e mudanças regulatórias como a Reforma Tributária são sinais claros de limite. Uma regra prática resume bem esse ponto: se crescer significa contratar mais gente para operar o sistema, e não para vender ou atender melhor, o momento chegou.

A substituição de um ERP costuma despertar receio na equipe por medo de errar, perder relevância ou enfrentar sobrecarga. Para não paralisar a rotina nem gerar atritos, a liderança precisa conduzir a migração como um projeto de negócio, e não apenas de TI. Isso exige o apoio visível da diretoria explicando os motivos da mudança, comunicação honesta e o envolvimento dos usuários-chave desde o início, pois quem participa do desenho compreende o resultado.

Na execução técnica, alguns cuidados garantem uma implantação segura. É fundamental estabelecer um escopo com prioridades claras para não resolver tudo de uma vez e revisar os processos antes da configuração, adotando as melhores práticas nativas da plataforma em vez de replicar vícios antigos. Customizações devem ser evitadas para não bloquear atualizações futuras, fazendo sentido apenas quando realmente giram o ponteiro do negócio.

Antes da virada (go-live), é preciso sanear cadastros e saldos, homologar cenários reais e escolher uma data fora de picos e longe de prazos fiscais críticos, garantindo para a equipe um plano de contingência e treinamento contínuo. Contar com uma consultoria especializada nesse trajeto oferece diagnóstico, domínio fiscal aplicado à realidade brasileira e transferência de conhecimento para que a empresa conquiste autonomia, e não dependência.

Após a entrada em operação, validar o retorno do investimento exige acompanhar, por pelo menos seis meses, métricas comparadas a uma linha de base prévia. Essa avaliação envolve eficiência operacional (fechamento contábil e ciclo pedido-faturamento), conformidade fiscal, resultados do negócio (giro de estoque e visibilidade de margem) e adoção interna, medida pelo uso efetivo dos recursos e recuperação da confiança da gestão nos números.

Para as PMEs que ainda hesitam, o conselho é não decidir no escuro: comece por um diagnóstico para medir o custo real das dores atuais, compare o risco de mudar com o risco de permanecer estagnado e avance em fases com escopo enxuto. Ao ouvir empresas semelhantes que já passaram pelo processo e enxergar a tecnologia como alavanca de crescimento, a organização cria a base necessária para escalar com segurança.

(*) Co-CEO da Okser.

24% dos consumidores brasileiros foram vítimas de golpes em compras online

Perdas médias de R$1.060,21 de acordo com pesquisa da Norton

Pesquisa revela que 53% dos brasileiros compraram de um suposto golpista porque a oferta era boa demais para deixar passar, enquanto metade (50%) dos que usaram um assistente de compras com IA afirma que ele recomendou ou concluiu uma compra de um varejista que não reconheciam na última temporada de festas de fim de ano.



pixelshot_CANVA

De acordo com o 2026 Norton Insights Report: Holiday Scams, 60% dos consumidores brasileiros estão mais preocupados com golpes online durante esta temporada de festas de fim de ano do que no ano passado. E há bons motivos para isso: 33% afirmam ter sido alvo de um golpe enquanto faziam compras online durante as festas de fim de ano, e 73% dos que foram alvos acabaram sendo vítimas.

Entre as principais conclusões do relatório estão:

- 24% dos consumidores brasileiros foram vítimas de um golpe enquanto faziam compras online durante as festas de fim de ano.
- 93% das vítimas de golpes perderam dinheiro, com uma perda média de R$1.060,21.
- 31% dos consumidores brasileiros afirmam que assumem mais riscos ao fazer compras online durante a temporada de festas de fim de ano do que em outras épocas do ano.
- 53% compraram em um site ou de um vendedor que suspeitavam que poderia ser um golpista porque a oferta era boa demais para deixar passar (Geração Z: 66%).
- 44% viram mais anúncios fraudulentos nas redes sociais do que no ano passado.
- 59% afirmam que a quantidade de conteúdo fraudulento e gerado por IA na internet fez com que ficassem mais cautelosos ao fazer compras online nesta temporada.
- 50% dos consumidores brasileiros que utilizaram ferramentas de compras com IA afirmam que, durante a última temporada de festas de fim de ano, uma dessas ferramentas recomendou ou concluiu uma compra em uma loja que não reconheciam.

Muitos consumidores brasileiros estão dispostos a assumir riscos por boas ofertas. O relatório revela que 74% afirmam que as ofertas influenciam suas decisões durante a temporada de festas de fim de ano, embora 64% desconfiem delas. Entre as pessoas entrevistadas:

- 68% comprariam em um site do qual nunca ouviram falar se o preço fosse atrativo.
- 50% arriscariam dinheiro em uma compra de um vendedor de quem suspeitam que possa ser um golpista. Em média, o valor máximo que arriscariam seria de R$372,20.
- 58% tomaram pelo menos uma medida arriscada para conseguir um presente muito procurado, como pagar muito acima do valor de mercado (28%), clicar em um anúncio em uma rede social ou em um e-mail (22%) ou comprar em um site desconhecido (16%).
- 47% chegaram a um site ou vendedor suspeito ao tentar comprar um artigo da moda, como um Labubu, Jellycat ou Copo Térmico Stanley.

"Os golpistas da temporada de festas de fim de ano não contam com o fato de que as pessoas sejam descuidadas. Contam com o fato de que as pessoas tenham pressa ou até mesmo estejam desesperadas para conseguir um presente muito procurado", afirma Iskander Sanchez-Rola, diretor sênior de IA e Inovação na Norton. "Quando parece que uma oferta pode desaparecer, até mesmo os compradores que suspeitam que algo está errado se arriscam. Essa diferença entre saber e agir é onde os golpistas obtêm seus lucros".

Anúncios fraudulentos são a principal fonte de golpes em compras de fim de ano

Entre os consumidores brasileiros que foram vítimas de golpes em compras de fim de ano, 55% afirmam ter sido enganados por meio de um anúncio fraudulento, 35% em uma plataforma de redes sociais, 33% em um site de terceiros, 25% por e-mail, 18% por telefone e 17% por mensagem de texto.

Alguns dos principais golpes relatados pelas vítimas brasileiras foram golpes em compras online (43%), golpes em plataformas de produtos usados ou de revenda (31%), phishing (24%) e golpes de entrega de encomendas (16%).

Dados dos Laboratórios de Ameaças da Gen: as lojas online falsas dobraram durante a temporada de festas de fim de ano de 2025

Durante a temporada de festas de fim de ano do ano passado, os produtos de segurança da família de marcas da Gen, incluindo a Norton, impediram mais de 46,7 milhões de tentativas de acesso a lojas online falsas em todo o mundo entre outubro e dezembro de 2025 — o equivalente a cerca de seis bloqueios por segundo. Durante esses três meses, a Gen bloqueou mais de 526.000 domínios da web associados a lojas falsas e protegeu mais de 16,6 milhões de pessoas em todo o mundo.

- As lojas falsas estão se multiplicando. A quantidade de domínios de lojas falsas bloqueados globalmente dobrou, passando de 260.000 durante o trimestre de festas de fim de ano de 2024 para 526.000 em 2025.
- As lojas falsas sobrevivem às festas de fim de ano. Entre as lojas falsas com mais bloqueios em 14 países, quase duas em cada três (64%) continuavam sendo bloqueadas seis meses após serem detectadas pela primeira vez.
- No Brasil, mais de 44.000 domínios foram bloqueados em 2025, um aumento de 96% em comparação com 2024.

"Anteriormente, criar uma loja falsa de comércio eletrônico exigia tempo e certos conhecimentos, mas, com a IA, os golpistas podem colocar em funcionamento uma loja falsa convincente em questão de minutos, com pouco ou nenhum investimento financeiro. Essa facilidade explica por que continuamos observando um aumento de lojas online falsas. Para os compradores, isso significa que um site com aparência profissional já não é prova de que se trata de um negócio legítimo; se você não procurou a loja por conta própria, vale a pena dedicar um tempo para pesquisá-la e confirmar que ela é legítima antes de concluir sua compra", diz Iskander Sanchez-Rola.

A IA está mudando os hábitos de compras online, mas nem sempre protege as pessoas contra golpes

Muitos consumidores brasileiros estão recorrendo cada vez mais à IA para apoiar suas compras de fim de ano, mesmo que não confiem plenamente que essas ferramentas os ajudem a evitar sites maliciosos. Embora 93% afirmem que usariam um assistente de compras com IA — uma porcentagem especialmente alta —, apenas 55% confiam que a ferramenta reconheceria e evitaria um site fraudulento. 72% já utilizaram um assistente ou agente de compras com IA, e 68% planejam usar uma ferramenta como o ChatGPT para fazer compras durante a temporada de festas de fim de ano.

Entre os brasileiros que utilizaram um assistente ou agente de compras com IA, 50% afirmam que, durante a temporada de festas de fim de ano mais recente, uma dessas ferramentas recomendou ou concluiu uma compra de um varejista que não reconheciam.

A Norton compartilha dicas para evitar golpes em compras online durante as festas de fim de ano

1. Verifique o site antes de comprar. Procure erros de digitação na URL, pesquise o nome da loja junto com os termos "golpe" ou "avaliações" e use uma ferramenta como o Norton Safe Web para detectar sites maliciosos.
2. Ignore o anúncio e acesse diretamente a loja. Digite o endereço da loja no navegador ou abra seu aplicativo oficial, em vez de clicar em um anúncio nas redes sociais.
3. Use proteção contra golpes baseada em IA. O Norton 360 Deluxe ajuda a detectar links fraudulentos, sites falsos e downloads maliciosos antes que causem danos. Seus recursos de proteção, incluindo o Safe AI, também ajudam a bloquear ações não autorizadas de ferramentas de IA, controlar o acesso aos seus arquivos pessoais e proteger contra links de risco.
4. Escolha métodos de pagamento com proteção. Use um cartão de crédito ou um serviço de pagamento com proteção ao comprador. Evite vendedores que solicitem transferências bancárias, cartões-presente ou criptomoedas.
5. Rastreie suas entregas pelos canais oficiais. Consulte o status da entrega no aplicativo da loja ou da transportadora, e não por meio de links incluídos em mensagens de texto ou e-mails.

O relatório completo 2026 Norton Insights Report: Holiday Scams está disponível (em inglês) em us.norton.com/blog/research/holiday-scams-insights-report-2026.