

Cinco dicas para proteger o setor financeiro de ataques cibernéticos

Especialista da Vericode alerta para riscos no ambiente digital e aponta práticas essenciais para garantir segurança, disponibilidade e confiabilidade operacional

No setor financeiro, a confiança é um ativo tão valioso quanto o próprio capital. Bancos, fintechs e corretoras operam diariamente com milhões de transações e dados sensíveis, em um ambiente cada vez mais digital, integrado e competitivo. Nesse contexto, qualquer falha em sistemas críticos pode resultar em prejuízos milionários, danos reputacionais e riscos regulatórios severos. O segmento lidera o ranking de incidentes cibernéticos no Brasil em 2025, concentrando 20,18% de todos os ataques registrados, segundo levantamento da ISH Tecnologia.

Além disso, o Relatório Global de Segurança na Nuvem 2024, da Check Point, aponta que incidentes em ambientes cloud cresceram de 24% em 2023 para 61% em 2024, um aumento de 154% em apenas um ano. Para Marcelo Marchi, CEO e sócio fundador da Vericode, especializada em qualidade de software, automação de testes e observabilidade, em um contexto de crescente dependência dos sistemas digitais para a continuidade dos negócios, a alta disponibilidade assume um papel estratégico. “Hoje, não se trata apenas de performance ou uptime, mas de resiliência operacional diante de falhas técnicas, ataques cibernéticos e picos inesperados de demanda”, afirma.

A seguir, o executivo elencou cinco dicas para proteger o setor financeiro de ataques cibernéticos:

1. Incorpore a segurança desde o início com uma cultura de DevSecOps
Falhas graves costumam surgir ainda na fase de desenvolvimento, quando a segurança é tratada apenas como uma etapa final. O DevSecOps é uma abordagem que integra desenvolvimento (Dev), segurança (Sec) e operações (Ops) desde o início do ciclo de criação de sistemas.

Ao antecipar a identificação de vulnerabilidades, as empresas reduzem riscos, ganham agilidade e evitam que problemas cheguem ao ambiente de produção. “Quando a segurança entra só no final, o custo do erro é sempre maior. O DevSecOps permite corrigir falhas ainda no código, antes que elas se tornem incidentes críticos”, destaca Marcelo Marchi.



2. Aposte em testes contínuos e automatizados

Testes manuais e pontuais já não são suficientes para sistemas financeiros complexos e altamente integrados. A automação de testes contínuos permite identificar falhas rapidamente e reduzir o risco de indisponibilidades. Plataformas como o dott.ai, da Vericode, utilizam Inteligência Artificial para executar testes de forma contínua, garantindo previsibilidade, qualidade de entrega e redução de custos operacionais sem comprometer a segurança.

3. Invista em observabilidade completa do ambiente

Acompanhar apenas logs já não é suficiente para garantir a estabilidade de sistemas financeiros complexos. Esses registros mostram o que aconteceu em um sistema, como erros, acessos e eventos, mas isoladamente oferecem uma visão limitada do funcionamento da operação. A observabilidade vai além do monitoramento tradicional ao reunir métricas de desempenho, rastreamento das transações e alertas inteligentes, criando uma visão integrada de todo o ambiente tecnológico.

Com essa abordagem, as equipes conseguem identificar comportamentos fora do padrão em tempo real, entender a origem dos problemas e agir antes que eles afetem clientes ou operações críticas. Para Marcelo Marchi, esse nível de visibilidade é decisivo: “Observabilidade não é só saber que algo falhou, mas entender rapidamente onde, por que falhou e qual será o impacto no negócio”, explica.

4. Aplique práticas de Site Reliability Engineering (SRE)

O Site Reliability Engineering (SRE) é uma abordagem que une engenharia e operação para garantir que sistemas críticos funcionem de forma estável,

previsível e escalável, mesmo sob pressão. Na prática, o SRE ajuda as empresas a inovar sem comprometer a confiabilidade dos serviços digitais. Dentro desse modelo, os SLOs (Service Level Objectives) funcionam como metas internas que indicam o nível ideal de disponibilidade, desempenho e tempo de resposta dos sistemas.

Já os SLAs (Service Level Agreements) são os compromissos formais assumidos com clientes, definindo o nível mínimo de serviço que deve ser entregue. Ao acompanhar esses indicadores de forma contínua, as empresas conseguem identificar riscos antes que eles se tornem falhas graves, priorizar correções e responder rapidamente a incidentes, mesmo em momentos de alta demanda ou durante ataques cibernéticos.

5. Controle custos e eficiência com FinOps

Em ambientes de nuvem, crescimento sem controle pode gerar desperdícios e riscos operacionais. O FinOps garante transparência, governança e otimização do uso de recursos, alinhando tecnologia e estratégia de negócio. Mais do que reduzir custos, essa disciplina assegura que investimentos em infraestrutura digital gerem retorno sustentável sem comprometer performance ou segurança.

Segundo Marcelo Marchi, falhas críticas não são inevitáveis, mas resultado de decisões mal estruturadas. “Empresas que investem em previsibilidade, observabilidade e segurança integrada conseguem antecipar problemas e manter a confiança do mercado, mesmo em um cenário de ataques constantes”, conclui.

Para mais informações, acesse: <https://vericode.com.br/pt>.

Planos de saúde empresariais baratos: economia que pode sair cara

José dos Santos Santana Júnior (*)

Nos últimos anos, muitos brasileiros passaram a buscar planos de saúde mais baratos como alternativa aos preços cada vez mais elevados dos contratos individuais

Nesse cenário, os chamados planos coletivos empresariais, especialmente os vinculados ao MEI, ganharam enorme popularidade. A lógica parece simples: abrir um CNPJ como microempregador individual e, com isso, acessar um plano empresarial com mensalidades significativamente menores. A proposta soa prática, rápida e econômica. E é justamente isso que atrai tantos consumidores.

O problema é que essa aparente solução esconde uma realidade pouco conhecida. O que muitos enxergam como um simples “atalho” para economizar pode, na prática, resultar em um dos maiores focos de conflito da saúde suplementar hoje: o chamado plano falso coletivo. Trata-se de contratos empresariais firmados sem a existência de um vínculo profissional real, situação comum quando o MEI é aberto exclusivamente para viabilizar a contratação do plano.

Os riscos costumam surgir com o passar do tempo. No início, o plano barato realmente parece vantajoso. No entanto, os planos coletivos empresariais, diferentemente dos individuais, não estão sujeitos aos limites de reajuste definidos pela Agência Nacional de Saúde Suplementar (ANS). Os aumentos são calculados com base no desempenho do grupo. Bastam algumas internações, cirurgias, exames ou tratamentos de maior complexidade para que o reajuste anual se torne completamente desproporcional. Há inúmeros relatos de famílias que começaram pagando cerca de R\$ 300 e, em poucos anos, passaram a arcar com mensalidades superiores a R\$ 900.

Outro ponto raramente destacado é o risco de cancelamento unilateral.

Como o contrato empresarial depende de um vínculo que, muitas vezes, não existe de fato, essa fragilidade pode ser utilizada pela operadora para rescindir o plano justamente quando ele se torna mais necessário. Consumidores em tratamento de doenças crônicas ou em uso contínuo de serviços descobrem, tardiamente, que o contrato pode ser encerrado sob o argumento de inexistência de uma empresa real que sustente o vínculo.

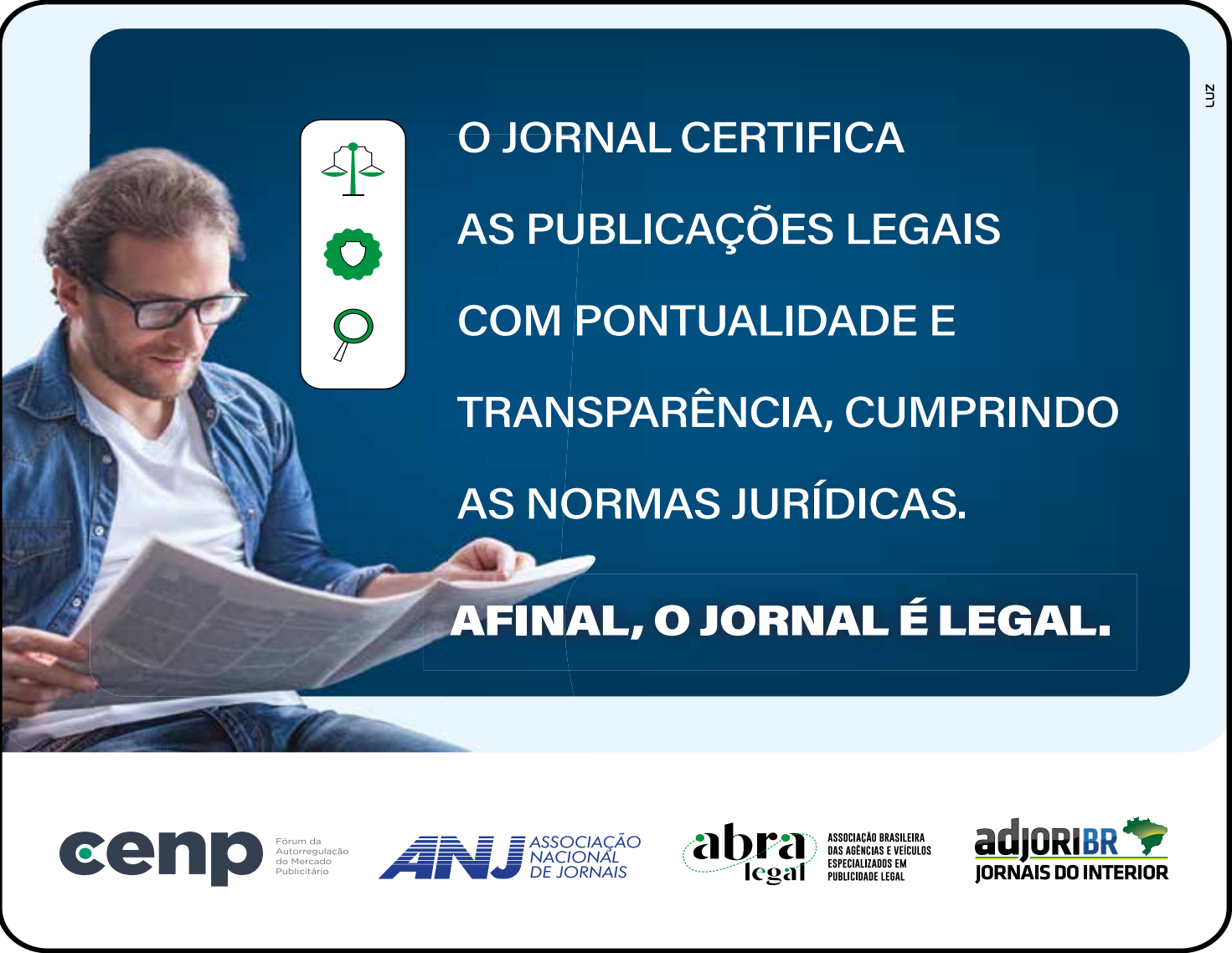
É por isso que especialistas alertam com insistência para os perigos do plano falso coletivo. Não se trata apenas de economia imediata, mas de segurança jurídica e assistencial no longo prazo. Um plano de saúde precisa ser estável, previsível e confiável, características que dificilmente estão presentes quando o contrato se apoia em uma relação empresarial artificial.

A boa notícia é que o Judiciário tem reconhecido que muitos consumidores são induzidos a esse tipo de contratação sem plena compreensão dos riscos envolvidos. Em diversas decisões, os tribunais têm reclassificado esses contratos como planos individuais quando fica demonstrado que o MEI não possui atividade econômica efetiva. Essa requalificação garante proteções que deveriam existir desde o início: controle de reajustes, manutenção da cobertura e, em alguns casos, devolução de valores cobrados indevidamente.

Por isso, antes de optar por um plano de saúde aparentemente mais barato na modalidade empresarial ou MEI, é fundamental refletir com cautela. Esses contratos não são, por si só, ilegais, mas podem se tornar altamente prejudiciais quando utilizados apenas para mascarar uma relação que não tem base real. A economia inicial pode custar caro no futuro, seja por aumentos imprevisíveis, insegurança contratual ou pelo cancelamento do plano no momento mais delicado da vida.

(*) Advogado especialista em Direito Empresarial e da Saúde e sócio do escritório Mariano Santana Sociedade de Advogados.

Edital de Intimação, prazo de 20 dias, Processo Nº 0002274-33.2025.8.26.0010. O MM. Juiz de Direito da 3ªVC, DO Foro Regional, x – Ipiranga, Estado de São Paulo, Dr. Carlos Antônio da Costa, na forma da lei, etc. Faz Saber a DANIELLE DOS SANTOS LIMA, CPF: 414.232.298-27, que diante da procedência e trânsito em julgado da ação Monitória Nº 1000490-77.2020.8.26.0010, foi proposta por parte de União Social Camiliana o incidente de Cumprimento de Sentença. Encontrando-se a ré, doravante executada, em lugar incerto e não sabido, foi determinada a sua intimação por edital para, no prazo de 15 (quinze) dias, a fluir após o prazo supra, pagar o débito exequendo de R\$ 16.797,42, corrigido monetariamente a partir de Junho/2025 e acrescido dos juros de mora a partir de Julho/2025, ficando advertida de que, transcorrido tal prazo sem o pagamento, será automaticamente iniciado o prazo de 15 (quinze) dias para apresentar impugnação independentemente de penhora ou de nova intimação (CPC, art. 525), e não ocorrendo pagamento o débito será acrescido de multa de 10% (dez por cento) e de honorários advocatícios de 10% (dez por cento), nos termos do art. 523 § 1º, do CPC, ficando também intimada para recolher as despesas judiciais de R\$ 779,68. Será o presente edital, por extrato, afixado e publicado na forma da lei. Nada Mais.



O JORNAL CERTIFICA
AS PUBLICAÇÕES LEGAIS
COM PONTUALIDADE E
TRANSPARÊNCIA, CUMPRINDO
AS NORMAS JURÍDICAS.
AFINAL, O JORNAL É LEGAL.



Fórum de
Autorregulação
do Mercado
Publicitário



ASSOCIAÇÃO
NACIONAL
DE JORNAIS



ASSOCIAÇÃO BRASILEIRA
DAS AGÊNCIAS E VEÍCULOS
ESPECIALIZADOS EM
PUBLICIDADE LEGAL



JORNAIS DO INTERIOR





PROTOCOLO DE ASSINATURA(S)

O documento acima foi proposto para assinatura digital na plataforma Certisign Assinaturas. Para verificar as assinaturas clique no link: <http://assinaturas.certisign.com.br/Verificar/85BB-4B5A-5C1C-408F> ou vá até o site <http://assinaturas.certisign.com.br> e utilize o código abaixo para verificar se este documento é válido.

Código para verificação: 85BB-4B5A-5C1C-408F



Hash do Documento

3605F49671A371CCFFE4FBA405727E0191C15A59587C268FB0A90F6B44CE63CA

O(s) nome(s) indicado(s) para assinatura, bem como seu(s) status em 16/01/2026 é(são) :

- ☒ Lilian Regina Mancuso - 05.687.343/0001-90 em 16/01/2026 19:08 UTC-03:00
- Tipo: Certificado Digital - JORNAL EMPRESAS E NEGOCIOS LTDA - 05.687.343/0001-90

Evidências

Geolocation: Location not shared by user.

IP: 172.16.4.6

AC: AC Certisign RFB G5

