

Sete estratégias para combater crimes digitais no mercado financeiro

Especialistas do setor financeiro explicam como enfrentar este desafio; estudo mostra que mais da metade dos brasileiros sofreu fraude em 2024

Os crimes digitais estão entre as maiores ameaças ao setor financeiro e de criptoativos. De acordo com relatório da Chainalysis, desde 2020, as estimativas anuais de atividades digitais ilícitas cresceram, em média, 25% ao ano. O relatório também mostra que os golpes digitais tenham desviado mais de US\$51 bilhões em 2024. No Brasil, a Serasa Experian aponta que 51% dos consumidores foram vítimas de fraude em 2024, e mais da metade sofreu perdas financeiras.

O avanço das tecnologias financeiras trouxe eficiência e inclusão, mas também abriu brechas para práticas ilícitas cada vez mais sofisticadas. Ataques de ransomware, fraudes envolvendo PIX e lavagem de dinheiro com criptoativos estão entre as modalidades mais frequentes.

Um estudo da IBM mostra que 97% das organizações que relataram um incidente de segurança relacionado à IA não possuíam controles adequados de acesso, 63% das organizações não tinham políticas de governança para gerenciar ou evitar a proliferação de IA invisível (shadow AI), e que o custo médio global de uma violação de dados pode chegar a US\$ 4 milhões.

"A resposta a esse cenário vai além de reforçar barreiras tecnológicas: exige integração entre setores, regulação adaptativa e, sobretudo, o desenvolvimento de soluções estruturais de compliance. É nesse ponto que especialistas destacam o papel de práticas como o compliance by design e a capacitação permanente como medidas de proteção indispensáveis para empresas e investidores", destaca o especialista em tecnologia financeira e CRO da infratech Azify, Gustavo Siuves.

Em janeiro de 2025, o Brasil registrou mais de 1,2 milhão de tentativas de fraude, alta de 41,6% em relação ao mesmo



mês de 2024, com destaque para o setor bancário, segundo dados do Serasa Experian.

"O combate aos crimes digitais exige mais do que tecnologia: requer uma cultura de compliance que antecipe riscos, integre controles desde a origem dos produtos e promova capacitação contínua. Na Azify, tratamos a segurança como um pilar estratégico, porque sabemos que proteger o ecossistema digital é proteger nossos clientes, parceiros e a reputação do mercado como um todo", destaca Elisa Plácido, Diretora de Compliance da Azify.

Sete estratégias para o combate ao crime digital financeiro

1. Compliance desde a concepção - O compliance by design propõe que controles de risco e prevenção a fraudes sejam incorporados desde a criação de produtos e serviços, e não apenas adicionados como camadas posteriores. Essa abordagem permite que qualquer operação financeira ou criptoativo já saia do zero com mecanismos de monitoramento integrados, minimizando vulnerabilidades. "O compliance precisa estar integrado já no desenho dos produtos, desde a concepção", explica Gustavo Siuves, CRO da Azify.

2. Capacitação contínua das equipes

O cenário digital evolui rapidamente, com novos tipos de ataques, ferramentas de anonimização e métodos de engenharia social. Treinar regularmente equipes de jurídico, auditoria, tecnologia e atendi-

ferramentas conseguem reduzir significativamente o tempo de resposta a incidentes.

5. Independência das áreas de compliance

- Para ser efetivo, o compliance deve atuar com autonomia em relação às áreas comerciais e de vendas. Decisões sobre bloqueio de contas, revisão de transações e investigação de atividades suspeitas não podem ser influenciadas por metas de negócio ou pressão por resultados financeiros. "A segurança dos clientes é prioridade máxima. Estruturamos controles para resistir a pressões externas, inclusive comerciais", reforça Siuves. Reguladores internacionais, como o FATF, também recomendam a separação de funções críticas para fortalecer a prevenção a crimes financeiros.

6. Regulação equilibrada e adaptativa - Embora a regulação seja essencial, medidas excessivamente restritivas podem gerar opacidade e deslocar operações para ambientes não regulamentados. O ideal é que existam regras proporcionais ao risco, combinadas com soluções de monitoramento tecnológico e controles internos robustos. Isso permite que o setor inove sem abrir espaço para atividades ilícitas.

7. Segurança como prioridade estratégica - Mais do que atender a exigências legais, empresas devem considerar a segurança digital como elemento central de sua estratégia. Isso envolve análise de riscos, simulações de ataques, auditorias regulares e monitoramento contínuo de operações, criando um ciclo de prevenção que protege clientes e fortalece a reputação institucional. "Inovação e proteção caminham juntas. Só assim podemos construir um mercado digital mais seguro e confiável", conclui Gustavo Siuves. Ao adotar essa mentalidade, as organizações conseguem não apenas reduzir prejuízos, mas também aumentar a confiança de investidores e parceiros estratégicos.

A revisão da ISO 9001 está chegando. O que esperar?

Anderson Farias (*)

A ISO 9001, a mais conhecida das normas ISO e referência mundial em gestão, passará por uma atualização com a publicação de uma nova versão em 2026

Essa revisão já era aguardada, pois a mais recente se deu em 2015 e o próprio modelo de gestão da ISO 9001 se baseia no conceito de melhoria, demandando ajustes frente às mudanças globais, avanços tecnológicos e demandas por maior clareza em sua aplicação.

As tendências que influenciam a revisão da norma refletem as transformações recentes no ambiente de negócios. A sustentabilidade a partir dos temas ambientais, sociais e de governança - ESG, aparece como tema central diante da pressão crescente exercida por investidores e reguladores. A gestão de riscos e a resiliência, especialmente após a pandemia e em meio a cenários geopolíticos instáveis, requerem um direcionamento estratégico mais sólido por parte das organizações. Além disso, a atualização normativa deverá considerar os avanços de digitalização e Indústria 4.0, incluindo automação, inteligência artificial, blockchain e internet das coisas (IoT), e em como as organizações lidam com estas aplicações em sua gestão.

Entre as mudanças previstas estão: maior envolvimento da alta direção e das lideranças, consolidando uma cultura de qualidade baseada em princípios éticos e práticas verificáveis; avanços na aplicação da mentalidade de risco, com exigência de mapeamento sistemático de riscos e oportunidades, além de uma preparação mais robusta para impactos externos inesperados; e a incorporação de competências digitais, abrangendo governança de dados, segurança da informação e confiabilidade dos registros digitais.

Para empresas já certificadas, a transição será significativa, mas menos disruptiva do que a versão de 2015. Ainda assim, será necessário um planejamento eficaz para alinhar os sistemas aos novos requisitos, agora mais estratégicos e conectados ao ambiente de negócios, com maior participação da alta direção e das lideranças. Os prazos de transição não foram definidos, mas deverão ocorrer em um ciclo de aproximadamente três anos após a publicação.

Mais que uma obrigação para organizações que optam pela certificação de sua gestão, a ISO 9001:2026 se consolidará como instrumento para fortalecer práticas de gestão, preparando organizações para enfrentar riscos globais e lidar com situações emergenciais em suas operações, respondendo adequadamente ao mercado.

(*) Consultor da Fundatec.

POLÍCIA PENAL DO ESTADO DE SÃO PAULO
COORDENADORIA DE REINTEGRAÇÃO SOCIAL E CIDADANIA
AVISO DE LICITAÇÃO

Encontra-se aberto na Divisão de Administração da Coordenadoria de Reintegração Social e Cidadania, o Edital de Pregão Eletrônico nº 00303/2025 - 05 - ASG 380247, critério de julgamento MENOR PREÇO, que tem por objeto a **Contratação de empresa para prestação de serviços técnicos para o programa CAEF Mulher e Diversidade**. A sessão pública será realizada no dia 07 de novembro de 2025, às 10:00 (horário de Brasília), por meio da plataforma Compras.gov.br: <https://www.gov.br/compras/pt-br>. O edital e seus anexos estarão disponíveis para consulta no endereço eletrônico: <https://pncp.gov.br/app/edital>. Maiores informações pelo e-mail: vaalexandre@sp.gov.br.

Proclamas de Casamentos

CARTÓRIO DE REGISTRO CIVIL

3º Subdistrito - Penha de França

Dr. Mario Luiz Migotto - Oficial Interino

Faço público a saber que: **KARIM DA SILVA FIORENTINO**, nascida em São Paulo, SP, em 19/06/2001, filha de Wagner Fiorentino e de Luciana Mara da Silva Fiorentino, nos termos do artigo 56 da Lei 6015/73 alterada pela Lei Federal 14.382/2022 promoveu a alteração do seu nome para: **KAREN DA SILVA FIORENTINO**.

Se alguém souber de algum impedimento, oponha-se na forma da lei. Lavro o presente,
para ser afixado no Oficial de Registro Civil e publicado na imprensa local
Jornal Empresas & Negócios

A man with a beard, wearing a grey suit and tie, is sitting and reading a newspaper. The background is blurred, showing other people in a public space.

TRANSPARÊNCIA

A TRANSPARÊNCIA
DA EMPRESA GERA
CONFIANÇA AOS LEITORES.
POR ISSO, AS PUBLICAÇÕES
LEGAIS NOS JORNAIS SÃO
ESSENCIAIS PARA A
SEGURANÇA JURÍDICA.

AFINAL, O JORNAL É LEGAL.

Fórum da 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: <https://assinaturas.certisign.com.br/Verificar/F499-2005-F6BA-290E> ou vá até o site <https://assinaturas.certisign.com.br:443> e utilize o código abaixo para verificar se este documento é válido.

Código para verificação: F499-2005-F6BA-290E



Hash do Documento

8470CCC9AE094B03B4BFDCF603A38B553F2A4BE3D88F388B2733E46895AF13F2

O(s) nome(s) indicado(s) para assinatura, bem como seu(s) status em 22/10/2025 é(são) :

- ☒ Lilian Regina Mancuso - 05.687.343/0001-90 em 22/10/2025 18:49 UTC-03:00
- Tipo:** Certificado Digital - JORNAL EMPRESAS E NEGOCIOS LTDA - 05.687.343/0001-90

