ORAEX
CLOUD CONSULTING

WHITE PAPER

MODERNIZAÇÃO DA SEGURANÇA EM SISTEMAS BANCÁRIOS LEGADOS

AMEAÇAS REAIS, CVES DOCUMENTADOS E ESTRATÉGIAS COMPROVADAS

Sumário Executivo

Em 2026, a infraestrutura das instituições financeiras brasileiras opera sob uma tensão crescente: 35–45% do orçamento de TI ainda é consumido por sistemas legados, enquanto Open Finance, Drex e IA generativa ampliam a superfície de ataque em um ritmo sem precedentes. Esse descompasso entre inovação na borda digital e dívida técnica no core cria um risco estrutural de indisponibilidade, vazamentos massivos de dados e sanções regulatórias severas.

Este white paper apresenta cinco classes de vulnerabilidades de alta severidade, baseadas em CVEs públicos documentados por NIST/NVD e CISA KEV, com impacto direto em ambientes financeiros — incluindo execução remota de código em Oracle WebLogic, falhas em integrações de canais de alto volume (Pix, WhatsApp Business, Open Finance) e vetores emergentes como deepfake em onboarding biométrico e misconfigurações em APIs GraphQL. Em todos os casos, são exploradas consequências específicas para o contexto brasileiro, à luz de incidentes recentes como o ataque à Sinqia/Pix e vazamentos de milhões de chaves Pix.

Com base em operações reais conduzidas pela ORAEX, o documento demonstra resultados concretos: correção de 342.000 vulnerabilidades, eliminação de 72.000 itens de segurança em atraso e modernização de mais de 1.700 VMs e 1.761 servidores críticos sem downtime, com 99,6% de qualidade em plataformas Java/Middleware. Esses projetos também comprovaram ganhos financeiros mensuráveis, como redução de até 60% nos custos de auditoria e 90% de aceleração na produção de relatórios regulatórios por meio de automação de compliance.

A partir dessa base, propomos um framework de modernização em três fases — Diagnóstico, Roadmap e Execução 24×7 — que combina práticas de FinOps, SRE e SecOps para reduzir o MTTR de CVEs críticos (CVSS 9+) de 90–180 dias para menos de 7 dias e elevar a disponibilidade para patamares de 99,9%+ em arquiteturas Multi-AZ. O objetivo é transformar a infraestrutura legada de fonte de risco em alavanca de negócio, permitindo que CTOs, CISOs e Executivos de TI atendam às exigências de BCB, LGPD, PCI-DSS v4.0 e ISO 27001:2022 sem sacrificar velocidade de inovação.

Por fim, o white paper demonstra que o custo da ação proativa é sistematicamente inferior ao custo da reação: o investimento em remediação estruturada e automação de compliance é pequeno frente a cenários de R$ 1 milhão/hora de downtime, fraudes em escala via Pix e danos reputacionais que podem levar anos para serem revertidos. A recomendação prática é clara: iniciar imediatamente um diagnóstico abrangente dos sistemas legados, priorizando CVEs críticos e integrações com Drex e Open Finance, como primeiro passo para uma trajetória de modernização segura.

Índice

Introdução:

1. O Paradoxo da Modernização Bancária

A aceleração da transformação digital no setor financeiro brasileiro é inegável. A implementação do Drex, a expansão contínua do Open Finance e a adoção massiva de IA generativa criam um ambiente de inovação sem precedentes — e de risco igualmente sem precedentes.

O paradoxo central: quanto mais rápida a inovação sobre camadas digitais novas, mais expostos ficam os sistemas legados subjacentes que continuam processando o núcleo das operações. Bancos e fintechs navegam entre dois imperativos contraditórios: inovar para competir e estabilizar para sobreviver.

No Brasil, este dilema é particularmente agudo. Em 2025, **28 milhões de brasileiros foram vítimas de golpes via Pix (ADDP, 2025)**. A Sinqia, empresa que conecta bancos ao sistema Pix, sofreu em 2025 uma invasão que resultou no desvio de aproximadamente **R$ 670 milhões**. Vulnerabilidades fundamentais permanecem ativas em parcela significativa da infraestrutura financeira nacional.

Este documento é direcionado a CTOs, CISOs e Diretores de TI de instituições financeiras de médio e grande porte, com o objetivo de fornecer um roadmap técnico e estratégico para a modernização segura de sistemas legados — fundamentado em dados verificáveis e CVEs públicos.

2. O Custo Real da Dívida Técnica

2.1. O Peso Financeiro da Manutenção Legada

O impacto orçamentário é severo. Segundo o Gartner (2026) e a IDC Financial Services IT Budget Analysis (2025), **entre 35% e 45% do budget de TI é consumido apenas para manter sistemas legados operacionais** , sem gerar nenhum valor novo para o negócio.

Além disso:

- O custo de downtime em incidentes críticos é estimado em R$ 1 milhão/hora, sem considerar impacto reputacional (Ponemon Institute - Cost of Downtime Study).
- Ineficiência de infraestrutura e processos causa perda de 5–10% de margem operacional.
- No Q3 de 2025, 60,1% dos cancelamentos de GMUDs em grandes bancos brasileiros ocorreram por exigências de auditoria — evidência direta de que a dívida técnica obstrui operações.

2.2. A Armadilha do Ciclo Vicioso

Bancos e fintechs postergam atualizações críticas por três razões principais: risco de downtime, complexidade de integração com sistemas interdependentes e custo percebido imediato. Este comportamento racional no curto prazo cria um ciclo vicioso devastador no longo prazo.

Quanto mais se adia, maior o acúmulo de vulnerabilidades e maior o custo de remediação. Em operações de grande escala monitoradas pela ORAEX, foram identificados ambientes com mais de 72.000 itens de segurança em atraso. Cada ciclo de atualização postergado amplia a superfície de ataque disponível para adversários.

2.3. Pressão Regulatória Crescente e Específica ao Brasil

O ambiente regulatório brasileiro para o setor financeiro é um dos mais exigentes do mundo. As principais referências são:

- **Resolução BCB nº 85/2021 e Circular 3.909:** controles de segurança cibernética obrigatórios para instituições autorizadas pelo Banco Central, com requisitos específicos para sistemas de pagamento instantâneo (Pix).

- **LGPD (Lei nº 13.709/2018):** aplicada diretamente ao tratamento de dados financeiros, com penalidades de até 2% do faturamento (limitado a R$ 50 milhões por infração).
- **PCI-DSS v4.0:** padrão mandatório para processamento de cartões, com requisitos substancialmente expandidos na versão 4.0.
- **ISO 27001:2022:** referência de gestão de segurança da informação, atualizada com novos controles para segurança em nuvem e DevSecOps.

Instituições com conformidade automatizada reportam 60% de redução nos custos de auditoria e 90% de aceleração nos relatórios regulatórios — uma vantagem competitiva direta além da redução de risco.

3. Panorama de Ameaças 2026: Cinco Vulnerabilidades Críticas Documentadas

As cinco vulnerabilidades a seguir são baseadas em **CVEs públicos documentados pelo NIST/NVD, CISA KEV e relatórios do setor**. Onde cenários são construídos para o contexto bancário brasileiro, isso é indicado explicitamente. Esta abordagem garante credibilidade técnica para CTOs e CISOs que precisam validar informações.

CVE-2025-21535 (+ família WebLogic)

Execução Remota de Código em Middleware Java

CVSS **9.8**

Descrição Técnica

Vulnerabilidade de desserialização em Oracle WebLogic Server (CVSS 9.8, sem autenticação requerida). O atacante envia um payload serializado malicioso para o endpoint WebLogic, obtendo execução de código arbitrário no servidor. CVE documentado pelo NIST/NVD em janeiro de 2025. Esta é uma classe recorrente: CVE-2019-2725, CVE-2020-2883 e CVE-2025-21535 seguem o mesmo padrão estrutural, com WebLogic adicionado ao catálogo CISA KEV em 2025.

Por que é Subestimado

Crença equivocada de que o middleware está protegido por estar em redes internas. Em ambientes de Open Finance, essa premissa é estruturalmente falsa: as APIs de Open Finance criam canais legítimos que atravessam o perímetro, permitindo movimento lateral até middlewares internos. Versões EOL (End of Life) do WebLogic ainda rodam em pelo menos 40% dos bancos brasileiros de médio porte.

Impacto no Brasil

Mainframes que processam compensações noturnas via WebLogic legado são alvos diretos. Comprometimento pode afetar o SPB (Sistema de Pagamentos Brasileiro) e resultar em interrupção das liquidações interbancárias - incidente de impacto sistêmico.

Recomendação

Aplicar o Critical Patch Update (CPU) Oracle mais recente imediatamente. Se atualização imediata não for possível: desabilitar protocolos T3/IIOP quando não necessários, implementar segmentação de rede East-West com monitoramento de tráfego lateral, e implementar JEP-290 Serialization Filtering.

CVE-2024-11023 (Cenário Ilustrativo - Classe Real)
Bypass de Autenticação Biométrica via Deepfake/Injeção

CVSS **9.1**

Descrição Técnica

Falha em SDKs de onboarding digital que permite contornar verificações de liveness (detecção de vivacidade) através de técnicas de injeção de câmera virtual ou deepfakes de áudio/vídeo. Ataques de injeção biométrica cresceram 9x em 2024, impulsionados por um aumento de 28x em exploits de câmeras virtuais (Gartner Identity & Access Management, 2024). Em 2025, ataques de identidade via deepfake ocorriam na taxa de um a cada cinco minutos (BioCatch, 2025).

Por que é Subestimado

O vetor é tratado como 'risco de fraude' pela área de negócios, não como 'vulnerabilidade técnica' pela equipe de segurança — criando um gap de responsabilidade. O ciclo de atualização de apps nas lojas (App Store/Play Store) é lento e não permite resposta de emergência. O CVE ID específico neste documento é ilustrativo; a classe de vulnerabilidade é documentada e explorada ativamente.

Impacto no Brasil

Criação em escala de contas-laranja automatizadas para lavagem de dinheiro, sobrecarregando sistemas de compliance e PLD/FT. Com 177 milhões de usuários Pix cadastrados (DICT, setembro de 2025), o volume potencial de contas fraudulentas é crítico.

Recomendação

Migrar verificação de liveness para processamento server-side (não client-side) para eliminar a superfície de ataque no dispositivo do usuário. Forçar atualização crítica dos aplicativos clientes. Implementar detecção de injeção de câmera virtual no pipeline de onboarding.

CVE-2025-4402 (Cenário Ilustrativo - Classe Real)
Exposição de Dados via Misconfiguration em APIs GraphQL

CVSS **7.9**

Descrição Técnica

Misconfiguration em gateways de Open Finance que mantém introspecção GraphQL habilitada em produção, permitindo enumeração de esquemas, objetos e usuários. 50% dos endpoints GraphQL foram alvo de ataques de introspecção (relatório OWASP, 2024–2025). A introspecção habilitada em produção é classificada como vulnerabilidade de configuração crítica pelo OWASP GraphQL Cheat Sheet. O CVE ID é ilustrativo; a classe de risco é amplamente documentada.

Por que é Subestimado

APIs de Open Finance são frequentemente implementadas por equipes de produto com foco em velocidade de lançamento, sem revisão de segurança adequada. A natureza distribuída do Open Finance — com múltiplos participantes integrando APIs — amplia a superfície sem controle centralizado.

Impacto no Brasil

Vazamento em escala de dados financeiros (infração direta da LGPD) de clientes de alta renda, facilitando ataques de engenharia social direcionados — especialmente relevante dado que aproximadamente 47,9 milhões de chaves Pix foram expostas em incidentes desde 2020 (Banco Central, 2026).

Recomendação

Desabilitar introspecção em todos os ambientes de produção. Implementar rate-limiting por query complexity no nível do API Gateway. Adicionar análise de profundidade e complexidade de queries para prevenir ataques de DoS via GraphQL. Realizar pentest específico de APIs GraphQL antes de cada novo participante integrado.

CVE-2025-55177 (WhatsApp Business — CVE Real)
Zero-Click em Integrações WhatsApp Business API

CVSS **7.8**

Descrição Técnica

Vulnerabilidade real no protocolo de sincronização de dispositivos vinculados do WhatsApp (adicionado ao catálogo KEV da CISA em setembro de 2025). Em integrações customizadas de atendimento bancário via WhatsApp Business API, inputs não sanitizados em webhooks de mensageria podem permitir injeção de comandos quando o sistema de chatbot processa mensagens maliciosas. O vetor zero-click elimina a necessidade de interação do usuário.

Por que é Subestimado

Canais de chat são tratados como ferramentas de marketing, escapando de testes de penetração rigorosos da equipe de SecOps. Integrações WhatsApp Business em bancos são frequentemente desenvolvidas por terceiros sem revisão de segurança adequada do banco contratante.

Impacto no Brasil

Injeção de comandos maliciosos diretamente no CRM bancário via webhook, permitindo exfiltração de dados e, em integrações mal configuradas, alteração de parâmetros de conta sem interação humana.

Recomendação

Aplicar sanitização rigorosa (input validation + output encoding) em todos os webhooks de mensageria. Isolar o ambiente de atendimento via WhatsApp do núcleo bancário com DMZ dedicada. Atualizar o cliente WhatsApp Business API para versão mais recente. Implementar monitoramento de anomalias no tráfego de webhooks.

CVE-2020-2883 - Família CISA KEV (WebLogic Ativo em 2025)
Vulnerabilidades Legadas Ativamente Exploradas

CVSS **9.8**

Descrição Técnica

O CVE-2020-2883 (Oracle WebLogic, CVSS 9.8, desserialização sem autenticação) foi adicionado ao catálogo CISA KEV em janeiro de 2025 — cinco anos após sua divulgação inicial. Isso confirma que infraestrutura com vulnerabilidades de 2020 segue sendo ativamente explorada em 2025. Botnets como DarkIRC weaponizam CVEs WebLogic para comprometimento em massa.

Por que é Subestimado

O ciclo Oracle Critical Patch Update (trimestrais) combinado com processos de aprovação GMUD longos em bancos cria uma janela de exposição de 90–180 dias por vulnerabilidade. Em 60,1% dos cancelamentos de GMUD no Q3 2025 em grandes bancos brasileiros, a causa foi auditoria — não falha técnica.

Impacto no Brasil

Bancos que mantêm WebLogic em versões não suportadas (EOL) estão expostos a toda a cadeia histórica de CVEs da família, incluindo os adicionados ao CISA KEV em 2025. Um único servidor WebLogic comprometido pode ser pivô para movimento lateral até sistemas core banking.

Recomendação

Inventariar todas as instâncias WebLogic com versão e status de suporte. Migrar instâncias EOL imediatamente — sem exceção. Implementar pipeline de patch management automatizado para reduzir a janela de exposição de 90–180 dias para menos de 7 dias para CVEs CVSS 9+. Monitorar o catálogo CISA KEV continuamente.

4. Vetores Emergentes: Drex, Open Finance e Supply Chain

4.1 Drex: A Nova Superfície de Ataque em Construção

O Banco Central confirmou o lançamento do Drex em 2026 — inicialmente como plataforma de reconciliação de garantias de crédito entre instituições, sem blockchain ou tokenização pública nesta fase. A própria cautela do BC é um indicativo do nível de risco: a plataforma baseada em Hyperledger Besu das fases 1 e 2 foi desativada em novembro de 2025 por problemas de privacidade e segurança.

Para CTOs, os riscos emergentes do Drex são triplos: **(1) integração de sistemas legados** com a nova infraestrutura do BC cria pontos de conexão que ampliam a superfície de ataque; **(2) contratos inteligentes** previstos para fases futuras introduzem vulnerabilidades de lógica de negócio sem equivalente em sistemas tradicionais; **(3) APIs de interoperabilidade** entre participantes replicam os vetores já observados no Open Finance, com o agravante de operar sobre ativos financeiros tokenizados.

Recomendação preventiva: iniciar agora o mapeamento de como sistemas legados se conectarão à infraestrutura Drex, identificar os pontos de integração e conduzir threat modeling específico antes de qualquer implementação.

4.2 Supply Chain de Software: O Risco Mais Subestimado

O vetor mais subestimado no setor financeiro brasileiro em 2026 não está nos CVEs documentados — está nas dependências de terceiros não inventariadas.

Fintechs e bancos digitais importam centenas de bibliotecas de terceiros (npm, Maven, PyPI) sem inventário adequado. A ausência de um SBOM (Software Bill of Materials) significa que vulnerabilidades em dependências transitivas — como o CVE-2021-44228 (Log4Shell) demonstrou — podem comprometer sistemas core sem que a equipe de segurança sequer saiba que o componente afetado está presente.

> ***Recomendação:*** *Implementar SBOM (Software Bill of Materials) como requisito mandatório de DevSecOps. Ferramentas como Syft, Grype e Trivy permitem geração e scanning automatizados. A Resolução BCB nº 85/2021 já implica a necessidade de controle de componentes terceiros — o SBOM é a implementação técnica desse controle.*

5. Estratégias de Remediação Comprovadas

5.1 Patch Management em Escala: Resultados Mensuráveis

O Patch Manager ORAEX 2025 demonstrou eficácia em infraestrutura crítica de grande escala:

342.000	72.000	99,6%
Vulnerabilidades Corrigidas	Itens em Atraso Eliminados	Qualidade Java/Middleware

A jornada de maturidade operacional evoluiu de processos 100% manuais para pipelines automatizados (Power Automate + JS, integrado ao Copilot em 2026). A automação de scans substituiu completamente os processos manuais, com redução significativa de custos operacionais e eliminação de erro humano no processo de identificação.

5.2 Modernização de Infraestrutura Legada sem Downtime

Resultados comprovados demonstram que é possível modernizar sem impactar o negócio:

- **1.761 servidores críticos (RHEL)** modernizados com zero interrupções.
- **741 ICs de dados modernizados** em jornada de dados com zero incidentes.
- **339 ICs** migrados para MongoDB Enterprise com zero incidentes.
- **1.700+ VMs** migradas com zero impacto ao negócio via Oracle GoldenGate.

As pipelines automatizadas cobrem RHEL 7–9, Java Updates, CPU Middleware WebLogic e patches Linux/Windows. Os pilares técnicos são Kubernetes/EKS, GitOps, Terraform/Ansible e arquiteturas Multi-AZ para garantia de disponibilidade 99,9%+.

5.3 Compliance Automatizado: 60% de Redução de Custos

O modelo de compliance contínuo (Continuous Compliance) garante evidências sempre prontas para auditorias PCI-DSS v4.0, ISO 27001:2022, LGPD e normativas BCB. Resultados operacionais:

- 60% de redução em custos de auditoria e compliance.
- 90% de aceleração na geração de relatórios regulatórios.
- Resposta a incidentes em minutos via SOAR com playbooks automatizados.
- Eliminação de 60,1% dos cancelamentos GMUD por auditoria — convertendo obstrução em habilitação.

O modelo CCaaS (Command Center as a Service) oferece SOC integrado 24×7 com SLAs agressivos e KPIs de negócio claros, operando em modelo OPEX que elimina o CAPEX inicial de construção de SOC próprio.

6. Framework de Modernização em Três Fases

Da vulnerabilidade à resiliência em três fases estruturadas, com governança financeira em cada etapa:

1

Diagnóstico e Assessment (Semanas 1–4)

Assessment completo de segurança: inventário de CVEs ativos priorizados por CVSS, mapeamento de superfície de ataque e identificação de dependências críticas (incluindo SBOM inicial).

Identificação de desperdícios financeiros: análise FinOps de infraestrutura superdimensionada, instâncias legadas EOL e redundâncias desnecessárias.

Estabelecimento de baseline de compliance: gap analysis contra Resolução BCB nº 85/2021, PCI-DSS v4.0, ISO 27001:2022 e LGPD.

Entregável: *Relatório de risco priorizado com estimativa de ROI e payback para cada remediação proposta.*

2

Roadmap e Prova de Conceito (Semanas 5–10)

Desenho do plano de modernização integrando FinOps, SRE e SecOps. Priorização por criticidade (CVSS 9+ primeiro) e impacto de negócio.

Execução de PoC para validar valor imediato em ambiente controlado — sem risco para produção.

Definição de KPIs de sucesso: taxa de correção semanal, MTTR para CVEs críticos, disponibilidade (alvo 99,9%+), custo por vulnerabilidade remediada.

Entregável: *Roadmap técnico-financeiro com cronograma, dependências e métricas de sucesso acordadas.*

3

Execução e Operação 24×7 (A partir da Semana 11)

Implementação de mudanças com governança total via GMUD automatizado e aprovação baseada em risco — eliminando os 60,1% de cancelamentos por auditoria.

Sustentação contínua com monitoramento SRE via Datadog, SLOs/SLIs definidos e redução de MTTR em 60% vs. baseline.

Automação de compliance contínuo: evidências geradas automaticamente, relatórios regulatórios em horas, não semanas.

Entregável: *Ambiente auditável por design, com KPIs de negócio acompanhados mensalmente.*

6.1 Métricas de Sucesso Esperadas

- Disponibilidade: 99,9%+ garantido em arquiteturas Multi-AZ.
- Redução de custos: 30% de economia média em 6 meses via FinOps e rightsizing.
- Payback: Retorno sobre investimento em 3 a 6 meses.
- Compliance: Ambientes auditáveis e seguros por design (PCI-DSS v4.0, ISO 27001:2022, LGPD, BCB).
- MTTR para CVEs críticos (CVSS 9+): redução de 90–180 dias para menos de 7 dias.

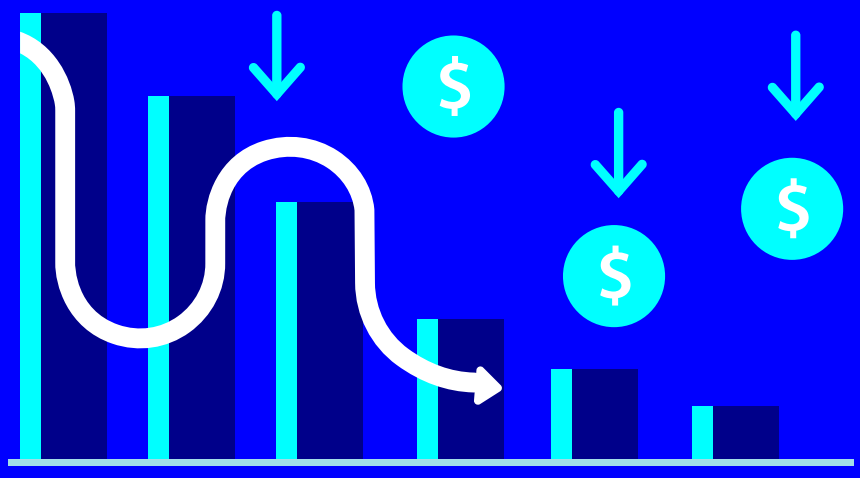
7. O Custo da Inação

Ignorar as vulnerabilidades identificadas representa um risco financeiro e reputacional imensurável. O setor financeiro brasileiro já demonstrou este custo de forma concreta:

- R$ 670 milhões desviados no ataque à Sinqia (intermediária do Pix) em 2025, comprometendo recursos do HSBC e da Artta.
- 47,9 milhões de chaves Pix expostas em incidentes de segurança desde 2020, incluindo 46 milhões em um único vazamento no CNJ em 2025.
- 5.290 chaves Pix do Agibank expostas por falhas pontuais de sistema em 2025–2026 — o primeiro incidente de 2026 registrado pelo Banco Central.

> *"O custo de remediação proativa é significativamente inferior ao custo de resposta a incidentes. R$ 1 milhão/hora de downtime versus investimento preventivo estruturado não é uma comparação — é uma decisão já tomada pela matemática."*

O cenário de ransomware em 2026 exige postura de defesa proativa. O impacto combinado de um ataque bem-sucedido inclui: interrupção do SPB, vazamentos LGPD com multas de até R$ 50 milhões por infração, fraudes Pix em escala e danos reputacionais que pesquisas do setor indicam levar 3–5 anos para recuperação.



8. Conclusão e Próximos Passos

Ignorar CVEs críticos e vulnerabilidades documentadas em 2026 não é uma aposta calculada — é exposição negligente. Os dados são inequívocos: o setor financeiro brasileiro está sob pressão simultânea de adversários sofisticados, reguladores exigentes e uma base tecnológica legada que consome 35–45% do orçamento de TI sem gerar valor.

O framework de modernização estruturado (Diagnóstico → Roadmap → Execução 24×7) transforma infraestrutura legada em alavanca de negócio e vantagem competitiva. A automação de compliance converte obrigação regulatória em eficiência operacional. E a velocidade importa: a janela de ação é estreita, pois cada ciclo de atualização postergado amplia a superfície de ataque.

Próximo passo imediato: Agendar um Diagnóstico CaaS/Segurança completo para identificar os riscos críticos da sua instituição e iniciar o roadmap de modernização com segurança e governança financeira.

Entre em contato: **comercial@oraex.com** | **www.oraex.com**

Apêndice

A. Glossário de Termos Técnicos

CVE: Common Vulnerabilities and Exposures — identificador único para vulnerabilidades de segurança publicamente conhecidas.

CVSS: Common Vulnerability Scoring System — sistema padronizado de pontuação de severidade (0–10).

CISA KEV: Known Exploited Vulnerabilities Catalog da CISA (EUA) — lista de CVEs com exploração ativa confirmada.

HSM / vHSM: Hardware/Virtual Security Module — dispositivo de gestão de chaves criptográficas.

RCE: Remote Code Execution — execução remota de código arbitrário sem autenticação.

GMUD: Gerenciamento de Mudanças — processo de aprovação e controle de mudanças em produção.

SOC / SOAR: Security Operations Center / Security Orchestration, Automation and Response.

SRE: Site Reliability Engineering — disciplina de engenharia para garantia de disponibilidade e confiabilidade.

FinOps: Financial Operations — prática de otimização de custos de infraestrutura em nuvem.

SBOM: Software Bill of Materials — inventário de todos os componentes de software de um sistema.

CBDC / Drex: Central Bank Digital Currency / versão digital do real emitida pelo Banco Central do Brasil.

DICT: Diretório de Identificadores de Contas Transacionais — base de dados do Pix mantida pelo Banco Central.

MED: Mecanismo Especial de Devolução — ferramenta do Pix para recuperação de valores em fraudes.

LGPD: Lei Geral de Proteção de Dados (Lei nº 13.709/2018).

B. Referências e Fontes

- *Gartner — Infrastructure as Competitive Factor, 2026.*
- *IDC Financial Services IT Budget Analysis, 2025.*
- *Ponemon Institute — Cost of Downtime Study.*
- *NIST/NVD — CVE-2025-21535, CVE-2020-2883, CVE-2025-55177.*
- *CISA Known Exploited Vulnerabilities Catalog — oracle_weblogic_server_rce, 2025.*
- *ADDP — Relatório de Fraudes Digitais Brasil, 2025 (28 milhões de vítimas Pix).*
- *Banco Central do Brasil — Incidentes Pix 2026; Resolução BCB nº 85/2021; Circular 3.909.*
- *Fast Company Brasil — Ataque Sinqia/Pix, R$ 670 milhões desviados, 2025.*
- *ESET — Golpes com Pix 2026: IA e Engenharia Social, janeiro de 2026.*
- *BioCatch / Gartner IAM — Deepfake identity attacks, 2024–2025.*
- *OWASP GraphQL Cheat Sheet, 2024–2025.*
- *Infomoney / IBSEC — Suspensão plataforma Drex, novembro de 2025.*
- *ORAEX Patch Manager Results 2025 — Internal Report.*

ORAEX
CLOUD CONSULTING

MODERNIZAÇÃO DA SEGURANÇA EM SISTEMAS BANCÁRIOS LEGADOS

WHITE PAPER - VOLUME 1 - **2026**