Opice Blum

Redefinindo os limites do possível.

cert.br nic.br cgi.br

Quem somos nós?

Time de Resposta a Incidentes · Opice Blum

Guilherme Ochsendorf de Freitas

Advogado Sênior · Time de Resposta a Incidentes · Auditor SIM3

Vinicius Azevedo

Advogado Gestor · Time de Resposta a Incidentes

Tiago Neves Furtado

Sócio · Proteção de Dados e Resposta a Incidentes

14º FÓRUM BRASILEIRO DE CSIRTs

Anatomia das Fraudes Financeiras

Vulnerabilidades, consequências e lições práticas para CSIRTs

São Paulo · 28 de julho de 2026

TLP:CLEAR

RESUMO

O que veremos

01 **Cenário das fraudes financeiras no Brasil**

Anatomia da fraude e a cadeia de ataque típica

02 **Identificação da causa raiz**

Credenciais expostas, ausência de MFA, APIs vulneráveis, privilégios excessivos, living-off-the-land, insiders e o padrão de maturidade SIM3

03 **Consequências**

ANPD, Bacen e responsabilidade civil e criminal

04 **Recomendações para CSIRTs**

O que muda no dia a dia do time de resposta

1 · CENÁRIO

Por que o sistema financeiro brasileiro virou alvo?

1 Motivação

- PIX permite transferência instantânea, irrevogável e em larga escala.
- Mercado brasileiro de fraude maduro: crime organizado financeiro com TTPs próprios.

2 Oportunidade

- Integrações financeiras complexas (BaaS, API gateways, Core Banking e Pagamentos).
- Superfície de ataque ampla e em constante mudança.

3 Racionalização

- Atacantes assumem que a vítima não vai reconstruir o ataque por falta de logs.
- Lacuna entre a obrigação regulatória e a capacidade real de comunicação tempestiva.

As fraudes mais relevantes não exploram uma vulnerabilidade isolada — elas encadeiam fragilidades estruturais.

1 · CENÁRIO

Anatomia de uma fraude financeira

A cadeia de ataque típica observada nos casos analisados

1

Reconhecimento

vazamentos prévios, aliciamento de colaboradores e mapeamento da infraestrutura exposta.

2

Acesso inicial

Credenciais vazadas, brute-force, phishing/vishing ou exploração de ativo exposto.

3

Escalada

Movimento lateral, abuso de privilégios excessivos e exfiltração de secrets internos.

4

Persistência

Criação de usuários e instalação de softwares legítimos (TeamViewer, AnyDesk, GetScreen).

5

Execução

Bypass dos controles da aplicação e chamada direta à API financeira (PIX, TED).

6

Monetização

Saques, transferências escalonadas e repasse para mulas e contas de terceiros.

2 · CASO A

Perdas estimadas em R$ 50 milhões

Como ocorreu?

1

Recrutamento de insider

Perfis no Telegram (**Plump Spider**) buscando funcionários das lojas.

2

Engenharia Social - Vishing

Colaboradores foram convencidos por telefone a instalar acesso remoto.

3

Living-off-the-land

AnyDesk, TeamViewer, GetScreen, fazendo movimentação letaral

4

Descoberta de credenciais senhas

"Codigos e senhas.txt" e o manual do Keycloak em pastas de rede (One Drive).

5

Execução e Apagão forense

Transferência (solicitando e aprovando) e exclusão conta de serviço apagando logs de Segurança, Sistema e PowerShell

AS FALHAS QUE VIABILIZARAM O INCIDENTE

- Falta de treinamento e orientação
- Sistemas transacionais (Sistema gestão de identidade e core bancário) sem MFA.
- Sem segregação de funções: requisitante e aprovador comprometidos.
- Centenas de transferências de R$ 300 mil a R$ 1 mi na madrugada, com destino a contas mulas.

POR QUE AS DEFESAS NÃO VIRAM

- Ferramenta de acesso remoto é software comercial e legítimo.
- Instalação autorizada pelo próprio funcionário.
- Nenhum malware customizado, nenhum zero-day: detecção por assinatura não tinha o que encontrar.

2 · CASO B

Perdas estimadas em R$ 43 milhões

Como ocorreu?

O INÍICIO: JENKINS CRIADO COM UMA IMAGEM COMPROMETIDA

- Uso de uma imagem Docker maliciosa/não oficial do Jenkins
- A imagem continha um backdoor persistente (oculto nas camadas do OverlayFS).
- Contêiner era executado como root e em privileged mode.

A ESCALADA: ACESSO INICIAL E CONTROLE DO AMBIENTE

- Acesso inicial aconteceu meses antes da fraude.
- O contêiner continha arquivos .env com tokens de acesso e segredos de produção.
- Acesso direto ao socket do Docker do host permitiu controlar o host.

O QUE ESTAVA EXPOSTO ALI DENTRO

- Senhas de bancos de dados produtivos em texto claro.
- Chaves de criptografia e tokens de APIs bancárias em .xml.
- Enumeração de clusters, buckets, tabelas, sub-redes e do AWS Secrets Manager.

O "PROXY FINANCEIRO"

1. Atacante

Controla a infraestrutura comprometida.

↓

2. Servidor confiável da empresa

Credenciais obtidas no Jenkins envia ordens com tokens válidos, IP conhecido e origem confiável.

↓

3. Banco parceiro

Aceita e processa as ordens como legítimas.

A fraude saiu de dentro da infraestrutura legítima da vítima.

2 · CASO C

R$ 9 milhões · mais de 6 mil clientes afetados em um dia

Como ocorreu?

1

Credencial legada

Access Key AWS de usuário desligado nunca revogada. Possível Info-stealer.

2

Cofre da nuvem e Mapeamento

Mapeamento, acesso ao AWS Secrets Manager, listou os cofres de backup exfiltração do arquivo kube/config.

3

Cluster Kubernetes

Acesso administrativo ao cluster sobre o orquestrador de contêineres. Chave privada RSA e master token da integração parceiro bancário (Banking as a Service)

4

Execução e Persistência

De posse dessas chaves e dos tokens das subcontas dos usuários o atacante passou a enviar ordens de transferência . Criação do usuário *natan-admin* para persistência

ONDE AS DEFESAS ESTAVAM CONCENTRADAS

- WAF e proteção de perímetro.
- Aplicação web e painel administrativo.
- Trilhas e validações da própria plataforma.

POR ONDE O ATACANTE PASSOU

- Envio direto à API do banco parceiro, com chaves válidas.
- Todo o investimento em defesa de perímetro tornou-se irrelevante.

Na data do incidente, os audit logs do Kubernetes e do banco de dados estavam desabilitados.

2 · SÍNTESE

O denominador comum

Quatro incidentes recorrentes — três deles com fator humano como principal causa

H

Senhas

Em arquivos de texto, planilhas e manuais deixados em pastas de rede.

H

Pessoas

Enganadas por telefone ou recrutadas em grupos de mensagem.

H

Treinamento

Desenvolvedor usando imagem não validada em servidores de automação e não revogou credencial.

T

Rastros

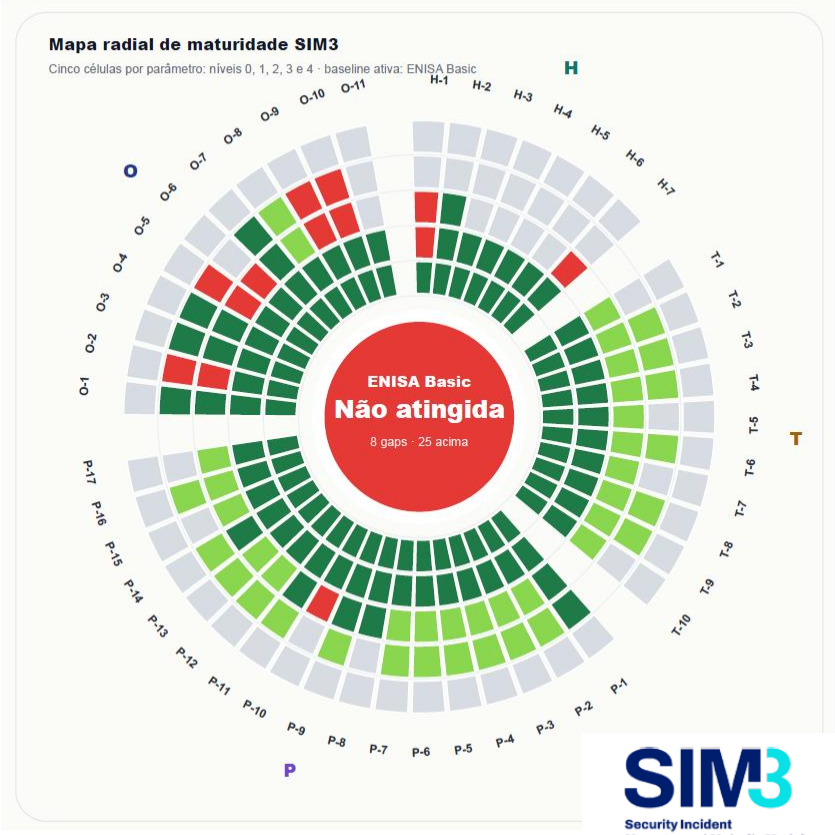
MFA desligado, audit logs inexistentes e eventos apagados.

H = fator humano · T = fator técnico

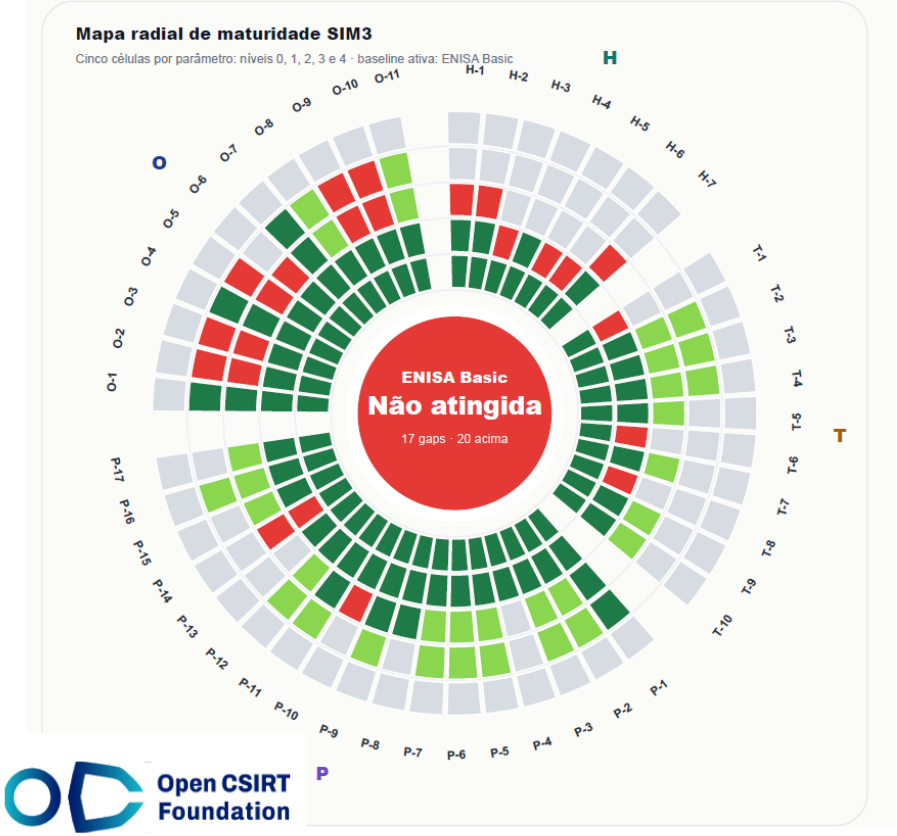
Nenhuma *das fraudes dependeu de zero-days ou de software hiper-sofisticado quebrando barreiras intransponíveis.*

Padrão de maturidade (SIM3)

Mapa radial ENISA Basic ·



Avaliação 1 · 8 gaps



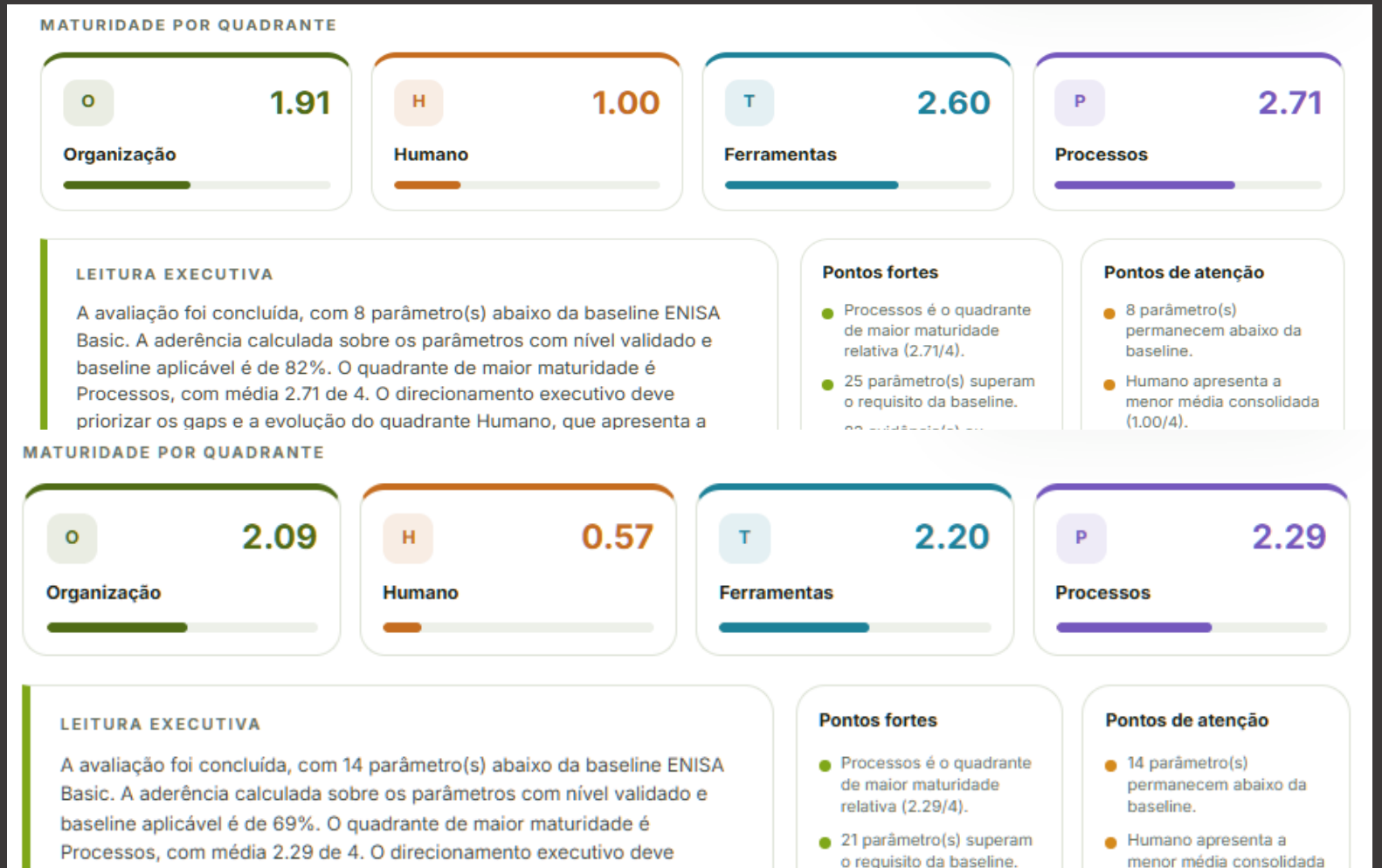
Avaliação 2 · 17 gaps

Security Incident Management Maturity Model · Open CSIRT Foundation

O elo menos valorizado continua sendo o humano

Maturidade por quadrante em duas avaliações — Humano é sistematicamente o menor

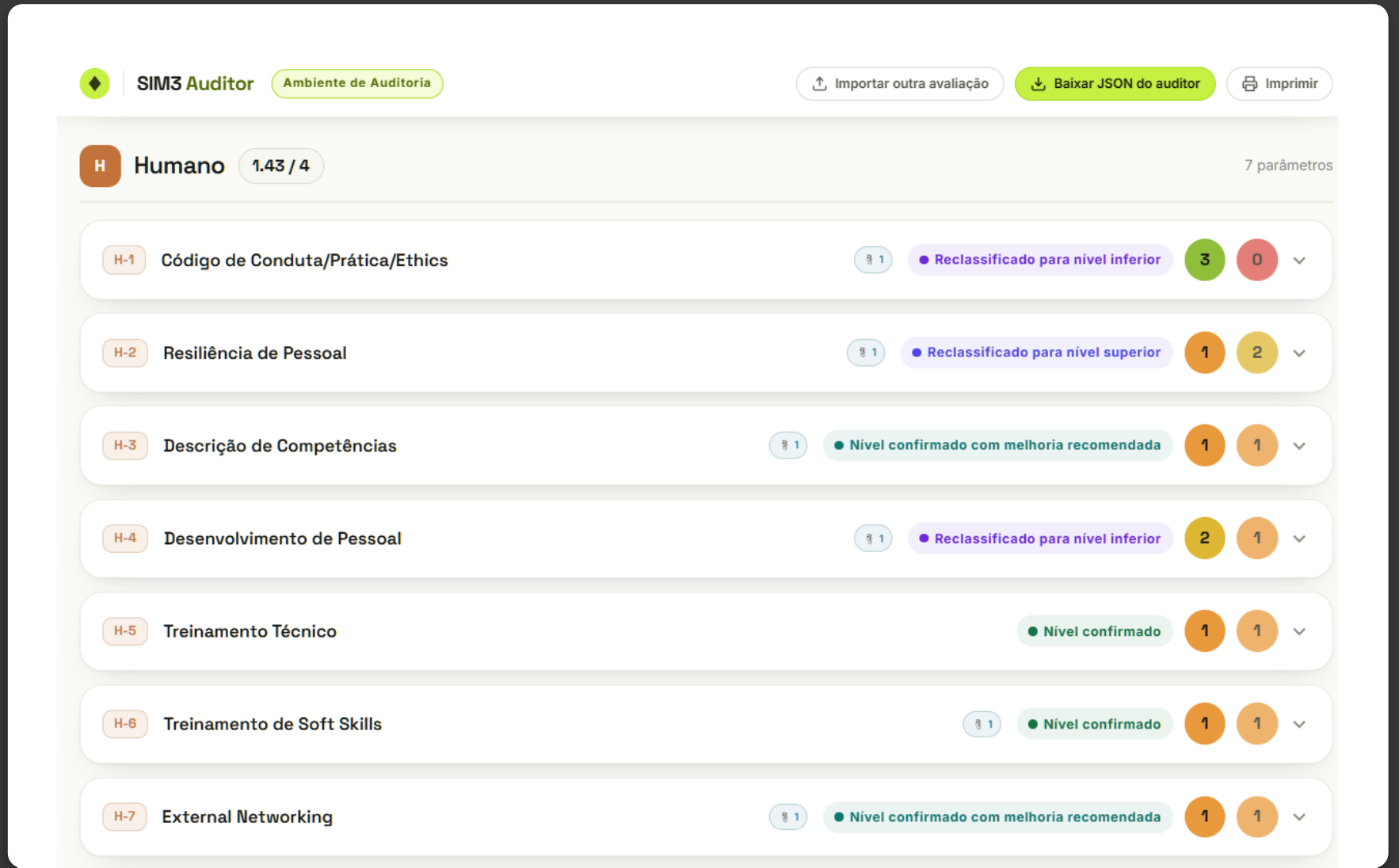
Padrão consistente: *processos e ferramentas são os quadrantes mais altos, e o investimento que falta é no quadrante humano.*



2 · MATURIDADE

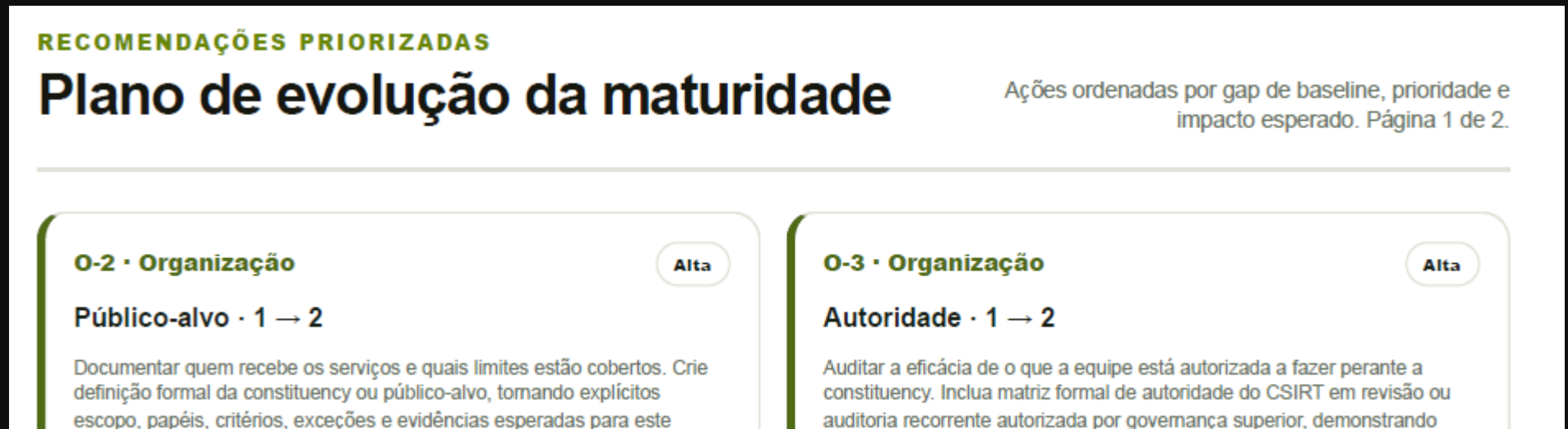
Quadrante Humano · detalhe da auditoria SIM3

Média consolidada 1.43 / 4 — o menor entre todos os quadrantes



Como as lacunas de maturidade aparecem nas fraudes

H-1	**Código de Conduta / Ética** Combate a insiders — o vetor central dos casos A e D.
H-6	**Soft Skills** Comunicação entre times, essencial na resposta coordenada.
P-13	**Outreach Process** Falta de incentivo a treinamento e conscientização junto ao público-alvo, que realimenta o problema humano.



RECOMENDAÇÕES PRIORIZADAS

Plano de evolução da maturidade

Ações ordenadas por gap de baseline, prioridade e impacto esperado. Página 1 de 2.

O-2 · Organização — Alta

Público-alvo · 1 → 2

Documentar quem recebe os serviços e quais limites estão cobertos. Crie definição formal da constituency ou público-alvo, tornando explícitos escopo, papéis, critérios, exceções e evidências esperadas para este

O-3 · Organização — Alta

Autoridade · 1 → 2

Auditar a eficácia de o que a equipe está autorizada a fazer perante a constituency. Inclua matriz formal de autoridade do CSIRT em revisão ou auditoria recorrente autorizada por governança superior, demonstrando

3 · CONEXÃO

O achado técnico define a decisão jurídica

Quatro dimensões técnicas, quatro decisões, quatro frentes de consequência

FATO TÉCNICO		DECISÃO JURÍDICA		CONSEQUÊNCIA
Linha do tempo	→	Prazo	→	**ANPD**
Escopo	→	Comunicação	→	**BCB**
Causa e controles	→	Responsabilidade	→	**Cível**
Logs e evidências	→	Estratégia probatória	→	**Criminal**

Quanto maior a incerteza técnica, maior a exposição jurídica.

3 · CONSEQUÊNCIAS

Uma fraude pode abrir quatro frentes simultâneas

O mesmo incidente gera obrigações distintas: a investigação técnica define o que se consegue demonstrar

ANPD

- Comunicação em 3 dias úteis, se houver risco relevante.
- Avaliação das medidas de segurança e da resposta.
- Sanções, se houver infração à LGPD.

Banco Central

- Comunicação de incidentes relevantes, conforme enquadramento.
- Resposta, continuidade e prevenção a fraudes.
- MED, bloqueio cautelar e mecanismos do PIX, quando aplicáveis.

Cível

- Restituição e indenização por prejuízos.
- Ações individuais, coletivas e demandas de terceiros.
- Demonstração de escopo, diligência e nexo causal.

Criminal

- Notícia-crime e preservação de evidências.
- Identificação de autores, insiders e fluxo financeiro.
- Subsídios à investigação e eventual responsabilização.

4 · RECOMENDAÇÕES

O que muda no dia a dia do time de resposta a incidentes?

1

Trate logs como ativo crítico

Retenção mínima de 6 meses, centralização no SIEM, integridade com hash e correlação por identidade. Audit logs de cluster, banco e API gateway são obrigatórios — sua ausência inverte o ônus da prova.

2

Invista no fator humano

Ferramentas avançadas não substituem equipe preparada. O quadrante Humano concentra as maiores lacunas: competências, treinamento, soft skills, comunicação e exercícios práticos.

3

Mitigação técnica é defesa regulatória

MFA universal em sistemas transacionais, cofre de senhas no IDP, segregação 4-eyes e bloqueio adaptativo. Cada controle pode afastar o dever de comunicação (Resolução 15/2024).

4

Integre Jurídico/DPO no playbook

Acionamento imediato e simultâneo. Membros com formação técnico-jurídica avaliam em paralelo causa raiz, escopo, hipótese legal e dever de comunicação, com templates de decisão documentada.

5

Documente cada passo por framework

Cada ação gera evidência: contenção, erradicação, recuperação e análise mapeadas contra NIST CSF 2.0 e ISO/IEC 27002:2022 — o laudo técnico se torna prova judicial.

PARTICIPE DA NOSSA PESQUISA

Radar Cyber & IA

Riscos cibernéticos, governança de IA e resposta a incidentes nas empresas brasileiras.

Radar Cyber & IA

Aponte a câmera do celular

Obrigado.

Tiago Neves Furtado
tiago.furtado@opiceblum.com.br

Vinicius Azevedo
vinicius.azevedo@opiceblum.com.br

Guilherme Ochsendorf de Freitas
guilherme.freitas@opiceblum.com.br