



CESCON BARRIEU

45º LIVE INTRA REDE

Cibersegurança: O Papel Essencial do Fator Humano

FRAUDES FINANCEIRAS E FATOR HUMANO

VULNERABILIDADES, CONSEQUÊNCIAS E
LIÇÕES PRÁTICAS PARA CSIRTs

Participante



GUILHERME OCHSENDORF DE FREITAS

Advogado Sênior, Especialista em Resposta a Incidentes e Cibersegurança no Cescon Barrieu.

Pós-graduado em Direito e Tecnologia pela POLI-USP e MBA em Gestão Estratégica de TI pela FEA-RP/USP. Professor em Cursos de Pós-Graduação em Direito Digital e Coautor de livros sobre o tema.

Certificações nacionais e internacionais, incluindo ISO/IEC 27001:2022 Lead Auditor, Certified SIM3 Auditor, certificações pelo ISC2 (CC) e Cisco (Cybersecurity Analyst), além do Incident Response Process Professional Certificate CERT® pela Carnegie Mellon University (CERT.br) e FGV.



<https://br.linkedin.com/in/guilhermeochsendorf>

O QUE VEREMOS

01

CENÁRIO DAS FRAUDES FINANCEIRAS NO BRASIL

Por que o sistema financeiro brasileiro virou alvo

02

IDENTIFICAÇÃO DA CAUSA RAIZ (FATOR HUMANO) E AVALIAÇÃO DE MATURIDADE SIM3

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 ADMINISTRADORES DE REDE

Controles práticos de rede, identidade e logs que teriam interrompido cada caso

01

CENÁRIO

Por que o sistema financeiro brasileiro virou alvo e como se estrutura uma fraude

POR QUE O SISTEMA FINANCEIRO BRASILEIRO VIROU ALVO?

01

MOTIVAÇÃO

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

02

OPORTUNIDADE

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

03

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.

02

CASOS REAIS E CAUSA RAIZ

2 incidentes, o denominador comum e o padrão de maturidade SIM3

PERDAS ESTIMADAS EM R\$ 50 MILHÕES

Como ocorreu?

01 Recrutamento de insider

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

02 Engenharia social · vishing

Colaboradores foram convencidos por telefone a instalar softwares de acesso remoto.

03 Living-off-the-land

Agente malicioso instalou AnyDesk, TeamViewer, GetScreen, e fez movimentação lateral.

04 Descoberta de credenciais

“Códigos e senhas.txt” e o manual do Keycloak em pastas de rede (OneDrive).

05 Execução e apagão forense

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

AS FALHAS QUE VIABILIZARAM O INCIDENTE

- Falta de treinamento e orientação.
- Sistemas transacionais (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 milhão 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.

R\$ 9 MILHÕES · MAIS DE 6 MIL CLIENTES AFETADOS EM UM DIA

Como ocorreu?

01 Credencial legada

Access Key AWS de usuário desligado por anos e nunca revogada. Como conseguiram a credencial? Possível info-stealer.

02 Cofre da nuvem e mapeamento

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

03 Cluster Kubernetes

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

04 Execução e persistência

Com essas chaves e os tokens das subcontas, 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.*

O DENOMINADOR COMUM

incidentes recorrentes — 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.

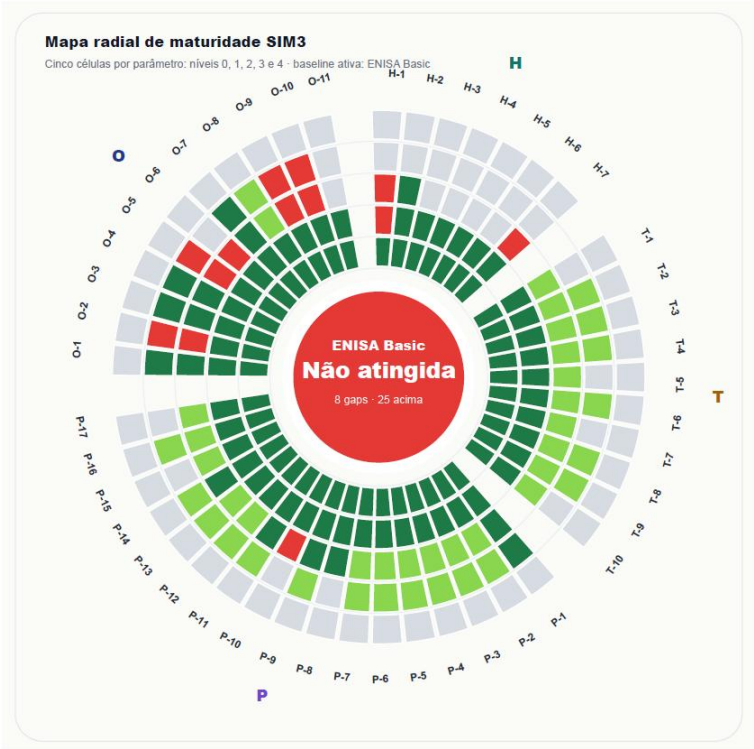
H = fator humano · T = fator técnico

Nenhuma das fraudes dependeu de zero-days ou de software hiper-sofisticado para praticar a fraude.

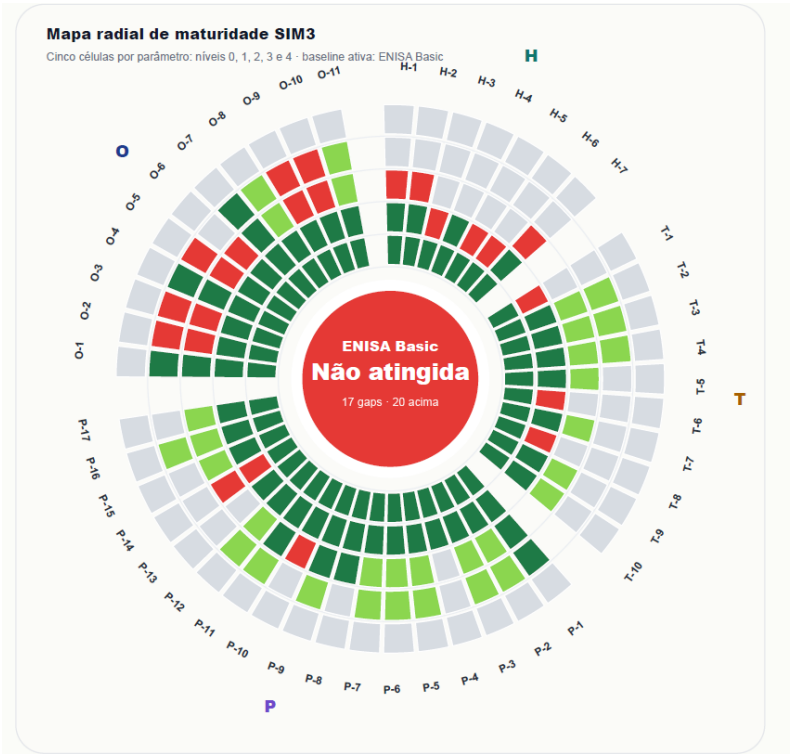
PADRÃO DE MATURIDADE (SIM3)

Security Incident Management Maturity Model · Open CSIRT Foundation

Mapa radial ENISA Basic



AVALIAÇÃO 1 · 8 GAPS



AVALIAÇÃO 2 · 17 GAPS

O ELO MENOS VALORIZADO CONTINUA SENDO O HUMANO

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



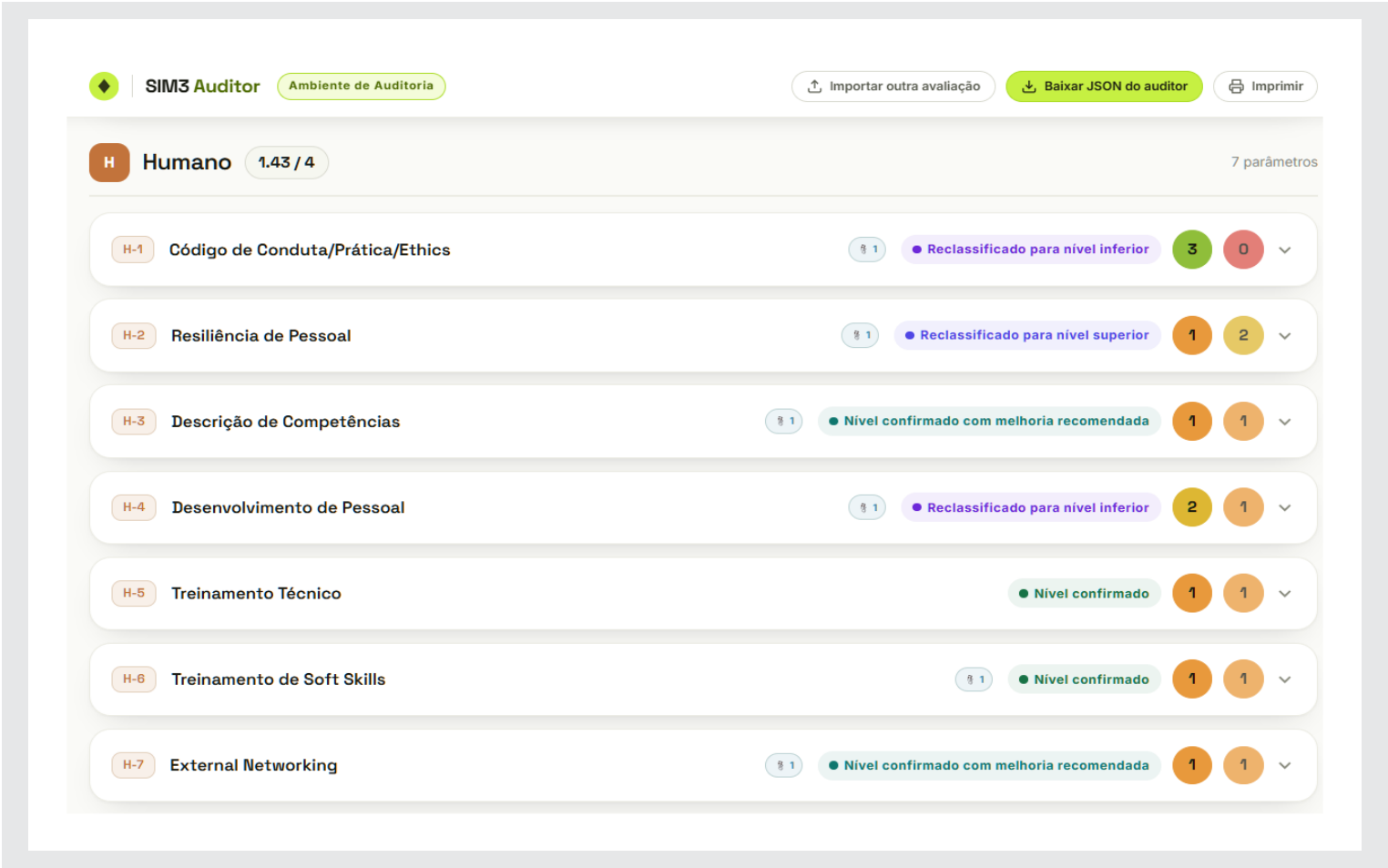
PADRÃO CONSISTENTE

Processos e ferramentas são os quadrantes mais altos, e o investimento que falta é no quadrante humano.

Médias por quadrante extraídas dos relatórios das duas avaliações SIM3.

QUADRANTE HUMANO · DETALHE DA AUDITORIA SIM3

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



03

CONSEQUÊNCIAS

Do achado técnico à decisão jurídica: ANPD, Banco Central, esfera cível e criminal

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.

04

RECOMENDAÇÕES

O que muda no dia a dia de quem administra a rede

O QUE MUDA NO DIA A DIA DE QUEM ADMINISTRA A REDE?

01

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 sempre habilitados — sem eles, não se reconstrói o ataque.

02

CONTROLE IDENTIDADES E ACESSOS

MFA universal em sistemas transacionais, cofre de senhas no IDP, segregação 4-eyes, menor privilégio para contas de serviço e revogação imediata de credenciais no desligamento.

03

INVISTA NO FATOR HUMANO E ACIONE CEDO

Treine equipes contra vishing e aliciamento. Ao suspeitar de incidente, acione CSIRT e Jurídico/DPO de imediato e documente cada ação (NIST CSF 2.0, ISO/IEC 27002:2022).

04

ENDUREÇA A INFRAESTRUTURA (HARDNING)

Somente imagens oficiais e validadas, contêineres sem root e sem privileged mode, socket do Docker nunca exposto e segredos fora de arquivos .env, .txt e pastas de rede.

05

CONTROLE O ACESSO REMOTO

Permita apenas ferramentas homologadas e bloqueie AnyDesk, TeamViewer, GetScreen e similares não autorizados. Alerta sobre instalações e conexões fora do padrão.

CESCON
BARRIEU

OBRIGADO.

45º LIVE INTRA REDE · CIBERSEGURANÇA: O PAPEL ESSENCIAL DO FATOR HUMANO

GUILHERME OCHSENDORF DE FREITAS



Av. Brigadeiro Faria Lima 949 10º and
Faria Lima Plaza
São Paulo - SP
T +55 11 3089 6500

Praia de Botafogo 228 15º and
Ed. Argentina
Rio de Janeiro - RJ
T +55 21 2196 9200

Rod. Stael Mary Bicalho Motta Magalhães
521 15º and
The Plaza
Belo Horizonte - MG
T +55 31 2519-2200

SH/Sul Quadra 06 Cj. A Bl. A Sala 506
Ed. Brasil 21
Brasília - DF
T +55 61 3030 1950

Avenida Tancredo Neves 620 Cj. 2119,
2120, 2121
Ed. Mundo Plaza
Salvador - BA
T +55 71 3039 4001

1 King Street W Suite 4800, 251
Toronto - ON
T +1 416-639-2132

Todos os direitos reservados. Esta apresentação não deverá ser divulgada ou distribuída para qualquer terceiro sem o consentimento prévio e expresso de Cescon, Barrieu, Fleisch & Barreto Advogados. Esta apresentação não constitui e não deve ser interpretada como aconselhamento legal, o qual deve ser obtido especificamente para qualquer atividade ou operação que se pretenda realizar. Não assumimos qualquer responsabilidade pela atualização das informações contidas nesta apresentação.

WWW.CESCONBARRIEU.COM.BR

TLP: CLEAR