RNP

Educação, Pesquisa
e Inovação em Rede

Gestão de Vulnerabilidades Baseada em Risco

Sobre

Especialista em Cibersegurança com mais de 15 anos de experiência em ambientes complexos, combinando bagagem sólida de infraestrutura a uma visão estratégica de segurança. Com passagem por grandes empresas como Raízen, EMS Farmacêutica e C&A, atua atualmente como Arquiteto de Segurança da Informação na RNP.

Certificado CEH, acumula histórico na liderança de resposta a incidentes, threat hunting, gestão de vulnerabilidades e operações de blue/red team. Possui ampla expertise na implementação de soluções robustas de MFA (para +8 mil usuários), SIEM, PAM, EDR e proteção em nuvem (Azure e GCP), destacando-se pelo alinhamento contínuo entre a segurança da informação e os objetivos do negócio.

Objetivos e Mapa da Apresentação

Esta apresentação cobre o ciclo completo da gestão de vulnerabilidades baseada em risco, do problema operacional ao modelo quantitativo, com critérios, fórmulas, exemplos calculados e métricas de governança. Cada módulo é autocontido e pode ser usado separadamente como referência técnica.

01

Descoberta e Normalização

Fontes, cobertura, deduplicação e consolidação de findings. CVE, CWE, CPE, ativos efêmeros e duplicidade entre scanners.

02

Categorização Técnica e por Camada

Taxonomia por natureza técnica (RCE, injeção, IAM, supply chain etc.) e por localização (endpoint, cloud, container, SaaS).

03

Enriquecimento Contextual

CVSS v4.0, EPSS, KEV, reachability, BIA, inventário técnico e cadeia de rastreabilidade de negócio.

04

Priorização e Modelos Quantitativos

Matriz P0–P3, modelo de score ponderado, modelo multiplicativo, exemplos calculados com entradas e saídas explícitas.

05

Remediação, Mitigação e Governança

Workflow operacional, SLA, virtual patching, controles compensatórios, aceite de risco, métricas e dashboard.

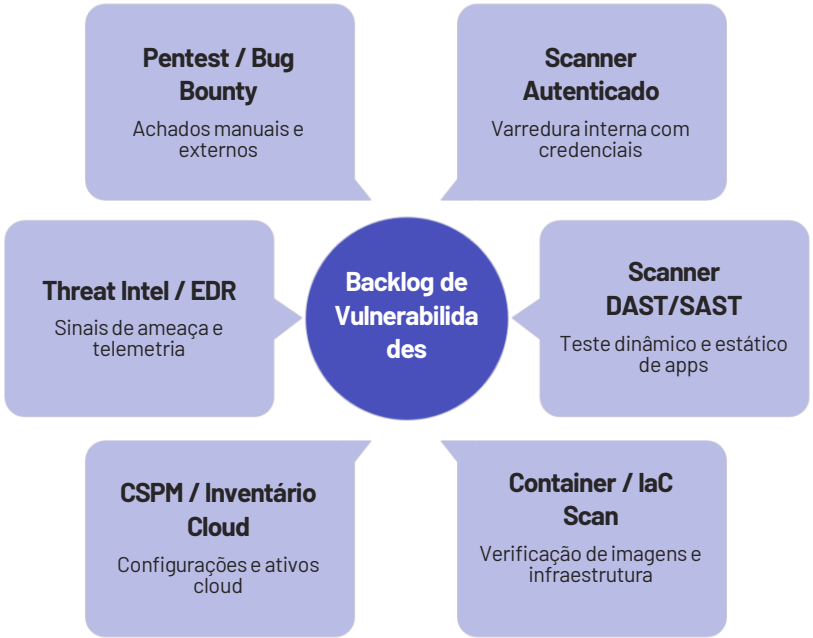
O Problema Real: Por Que o Backlog Cresce

A maioria das organizações não enfrenta um problema de descoberta — enfrenta um problema de sobrecarga de signal sem contexto suficiente para decidir. O backlog cresce não porque o scanner falha, mas porque o processo depois do scan é disfuncional.

Causas Estruturais do Backlog

- **Volume:** scanners modernos geram dezenas de milhares de findings por ciclo em ambientes médios; sem triagem automatizada, a fila é impossível de gerir manualmente.
- **Duplicidade:** o mesmo CVE em um ativo pode aparecer em três scanners distintos com severidades diferentes e estado diferente (open/fixed).
- **Findings sem owner:** ativos sem CMDB atualizado não têm responsável definido; o finding fica em limbo indefinidamente.
- **Ativos desconhecidos:** shadow IT, cloud accounts não inventariadas, containers efêmeros e pipelines de CI/CD criam pontos cegos estruturais.
- **Visões inconsistentes:** scanner A detecta CVE-XXXX via banner, scanner B detecta via fingerprint de pacote — saídas divergem em status e versão.
- **Vulnerabilidades transitivas:** dependências de terceiro nível em SCA que não afetam o código em execução mas aparecem como críticas no relatório.
- **Falsos positivos:** pacotes presentes mas não executáveis, versões parcheadas sem atualização de metadados, sistemas com backport sem CVE atualizado.
- **Ativos efêmeros:** containers imutáveis recriados a cada deploy invalidam remediações; a vulnerabilidade retorna a cada pipeline.
- **Fadiga de alertas:** equipes param de reagir quando o volume é desproporcional à capacidade de resposta.

Fluxo de Ingestão Multi-Fonte



Conceitos que Não Podem Ser Confundidos

Confundir terminologia gera decisões erradas. Um gestor que trata "CVSS alto" como sinônimo de "risco alto" irá priorizar incorretamente. A tabela abaixo define cada termo com precisão operacional.

Termo	Definição Operacional	Exemplo
Vulnerabilidade	Fraqueza técnica em software, configuração ou processo que pode ser explorada.	Buffer overflow em biblioteca de parsing de XML.
Ameaça	Agente ou evento com potencial de explorar uma vulnerabilidade.	Grupo de ransomware com TTPs documentados.
Exploit	Código ou técnica que concretiza a exploração da vulnerabilidade.	PoC público no GitHub ou módulo Metasploit.
Exposição	Condição que torna o ativo alcançável pelo vetor de ataque.	Serviço exposto na internet sem autenticação.
Probabilidade	Estimativa de que a vulnerabilidade seja explorada em um horizonte temporal.	EPSS 0,72 = 72% de probabilidade em 30 dias (estimativa do modelo).
Impacto	Consequência para confidencialidade, integridade, disponibilidade ou negócio.	RCE em servidor de pagamentos = impacto financeiro e regulatório.
Risco	Função de probabilidade × impacto, contextualizada ao ambiente.	CVSS 8,5 + EPSS baixo + ativo isolado = risco baixo.
Controle	Medida que reduz probabilidade ou impacto.	WAF bloqueando vetor de injeção, MFA em identidade privilegiada.
Risco Residual	Risco remanescente após aplicação de controles.	Falha sem patch com WAF ativo: risco reduzido, não eliminado.

Caso A — CVSS 9,8 sem caminho de ataque

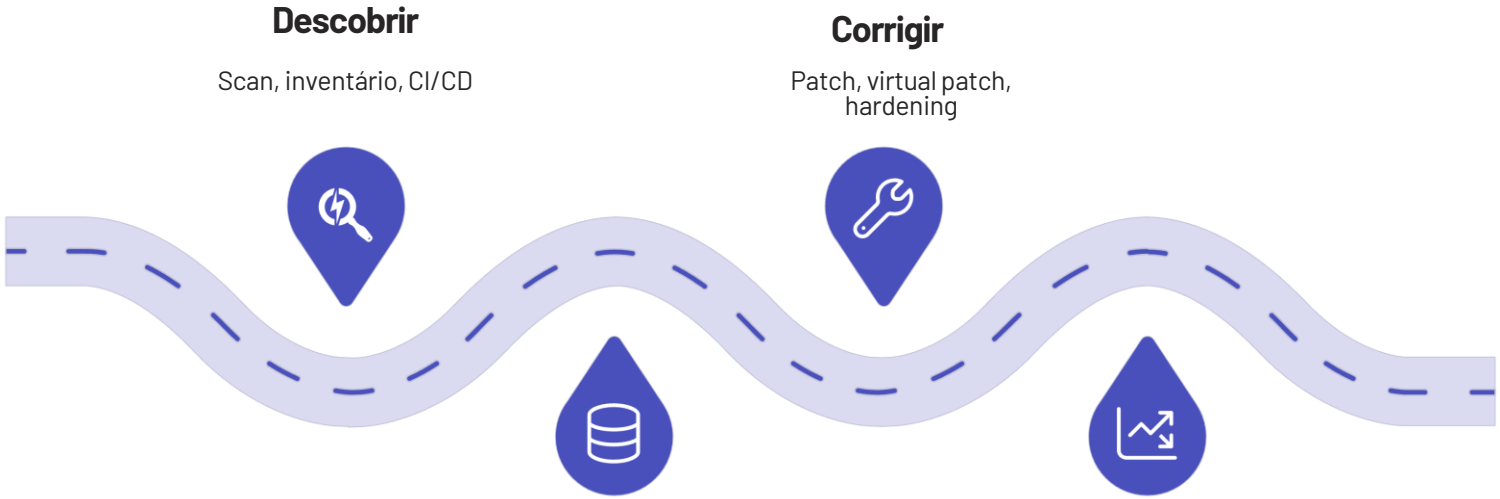
Falha de RCE em biblioteca não exposta, em ativo air-gapped, sem rota de entrada e sem exploit público. CVSS alto, risco contextual baixo. Ação: correção planejada no próximo ciclo.

Caso B — CVSS 5,3 com caminho de exploração real

Falha de autenticação bypass em API pública, KEV confirmado, EPSS alto, dados pessoais acessíveis. CVSS moderado, risco real alto. Ação: P0 imediato, mitigação em horas.

Ciclo de Vida Completo da Gestão de Vulnerabilidades

O ciclo não é linear em produção — ativos novos entram continuamente, patches falham, vulnerabilidades reaparecem e controles compensatórios expiram. Cada etapa possui entradas, decisões obrigatórias e evidências que devem ser registradas para fins de auditoria e governança.



Entradas e Decisões Críticas

- **Validar :** falso positivo deve ser documentado com justificativa técnica, não descartado silenciosamente.
- **Enriquecer :** sem BIA e reachability, a priorização é incompleta e potencialmente enganosa.
- **Atribuir :** finding sem owner é finding sem SLA. A ausência de owner deve disparar escalação automática.

Evidências Obrigatórias por Etapa

- **Descoberta:** timestamp, fonte, versão do scanner, asset_id.
- **Priorização:** score calculado, modelo utilizado, premissas e overrides manuais registrados.
- **Fechamento:** evidência técnica de remediação (log de patch, print de scan pós-fix, ticket de change).
- **Monitoramento:** data de última verificação, controle ativo e prazo de revisão de risco residual.

Fontes de Descoberta e Suas Limitações

Nenhuma fonte única cobre todo o ambiente. A combinação de fontes aumenta cobertura, mas introduz duplicidade, inconsistência de versão e conflitos de status. O time de VM deve entender a profundidade e a latência de cada ferramenta antes de confiar nos dados.

Scanner Autenticado vs. Não Autenticado

Autenticado: acesso ao sistema via credencial; detecta pacotes instalados, versões, configurações e ausência de patches. Alta precisão, cobertura profunda. Risco: credenciais armazenadas no scanner.
Não autenticado: fingerprint de banner, portas abertas e respostas de serviço. Menor precisão, mais falsos positivos. Útil para cobertura de ativos desconhecidos.

SAST, DAST e SCA

SAST: análise de código-fonte; encontra falhas de lógica, injeção, criptografia fraca. Alta latência (integrado ao CI). Muitos falsos positivos sem tuning.
DAST: testa a aplicação em execução; identifica comportamentos reais mas não vê código interno.
SCA: analisa dependências; vulnerabilidades transitivas podem não ser alcançáveis em runtime.

Container, IaC e CSPM

Container scanning: analisa imagem base e pacotes; resultados ficam desatualizados assim que a imagem é reconstruída. Ativos efêmeros exigem integração com pipeline.
IaC: detecta misconfigurações antes do deploy (Terraform, CloudFormation).
CSPM: monitora configuração de cloud em runtime; complementa IaC com visão de drift.

ASM, EDR, Pentest e Threat Intel

ASM/EASM: descobre ativos externos desconhecidos; alta latência, visão de attacker.
EDR: telemetria de endpoint; detecta comportamento de exploit em runtime.
Pentest/Bug bounty: validação humana; baixa frequência, alta confiabilidade.
Threat intel: contextualiza exploração ativa de CVEs no setor; não substitui scan técnico.

⚠ Duplicidade entre fontes é inevitável. Sem normalização, o mesmo finding aparece múltiplas vezes com prioridades conflitantes, inflando o backlog artificialmente.

Normalização e Deduplicação

O objetivo da normalização é consolidar múltiplos findings de múltiplas fontes em um único problema remediável, mantendo rastreabilidade de todas as evidências originais. Sem esse passo, o backlog é uma lista de eventos, não uma lista de trabalho.

Identificadores Padrão

- **CVE (Common Vulnerabilities and Exposures):** identificador único de vulnerabilidade mantido pelo MITRE/NVD. Base de correlação entre fontes.
- **CWE (Common Weakness Enumeration):** classifica a natureza técnica da fraqueza (ex.: CWE-79 = XSS, CWE-89 = SQL Injection). Orienta taxonomia e remediation patterns.
- **CPE (Common Platform Enumeration):** identifica produto/versão afetado. Permite mapear CVE a ativos por versão de pacote ou sistema operacional.
- **Package + Version + Image Hash:** em ambientes container, o CPE pode ser insuficiente; o hash da imagem é mais preciso.
- **Asset ID + Cloud Resource ARN/ID:** âncora do finding ao inventário de ativos.

Chave de Deduplicação

A regra de deduplicação canônica combina: `CVE_ID + asset_id + package_version + attack_vector`. Findings da mesma tupla são agrupados como instâncias do mesmo problema, preservando metadados de todas as fontes originais.

Exemplo de Deduplicação

Campo	Scanner A	Scanner B	Resultado Normalizado
CVE	CVE-2024-XXXX	CVE-2024-XXXX	CVE-2024-XXXX
Asset ID	srv-prod-042	srv-prod-042	srv-prod-042
Pacote	openssl 3.0.7	openssl 3.0.7	openssl 3.0.7
Vetor	Network	Network	Network
Severidade	CVSS 7,5	CVSS 8,1	CVSS 7,5 (NVD oficial)
Status	Open	Open	Open — 2 evidências
Ação	—	—	1 finding consolidado

Preservar evidências originais permite auditoria e detectar divergências entre ferramentas ao longo do tempo.

Casos Especiais

- **Backport:** distribuição Linux aplica patch de segurança sem atualizar número de versão; scanner pode reportar falso positivo. Validar via changelog ou aviso do vendor.
- **Container imutável:** finding persiste até rebuild da imagem. O problema remediável é a imagem base, não o container em execução.
- **Vulnerabilidade sem CVE:** misconfigurações, secrets expostos e fraquezas de processo; usar CWE + ID interno de política.

Categorização por Natureza Técnica

A taxonomia técnica orienta o tipo de correção, a equipe responsável e o padrão de impacto esperado. Uma categoria bem definida permite criar runbooks específicos e métricas de recorrência por classe de fraqueza.

Categoria	Exemplos Técnicos	Impacto Típico	Evidência Primária	Equipe Owner
RCE	Buffer overflow, desserialização insegura, template injection	Comprometimento total do host	PoC executado, saída de código remoto	Infra / App Security
Injeção	SQL injection, command injection, LDAP injection (CWE-89, CWE-77)	Exfiltração de dados, execução de comandos	Payload de teste, log de query	AppSec / Dev
Autenticação	Bypass de MFA, credencial padrão, token sem expiração	Acesso não autorizado a contas privilegiadas	Log de autenticação, teste funcional	IAM / AppSec
Autorização	IDOR, privilege escalation, path traversal (CWE-22, CWE-284)	Acesso a dados de outros usuários ou escalada	Resposta HTTP com dados de outro usuário	AppSec / Dev
Exposição de Dados	PII em log, chave em resposta de API, bucket S3 público	Violação regulatória (LGPD/GDPR), vazamento	Dado sensível em resposta, DLP alert	AppSec / Cloud / Compliance
Criptografia	TLS 1.0, cipher fraco, chave hardcoded, hash MD5	Interceptação, decodificação de tráfego	Resultado de sslyze/testssl, análise de código	Infra / AppSec
Configuração	Porta desnecessária aberta, admin sem senha, debug ativo em produção	Vetor de acesso inicial, exposição de informação	CSPM alert, scan de configuração	Infra / Cloud / DevOps
Dependência / Supply Chain	Pacote NPM malicioso, biblioteca com CVE, typosquatting	Comprometimento silencioso do pipeline ou runtime	SCA report, hash de pacote verificado	Dev / AppSec / DevSecOps
IAM / Identidade	Role com permissão wildcard, service account com admin global	Lateral movement, escalada de privilégio em cloud	IAM policy review, CSPM finding	IAM / Cloud Security
Segredo Exposto	API key em repositório, senha em variável de ambiente, secret em imagem	Acesso imediato a sistema ou dado; difícil de revogar post-facto	Secret scanner (Trufflehog, Gitleaks), CSPM	Dev / DevSecOps
Kernel / Container	Escape de container, privilege escalation de kernel (ex.: dirty pipe)	Comprometimento do host subjacente a partir de container	PoC de escape, kernel version check	Infra / Platform
Firmware / OT	Firmware desatualizado em dispositivo IoT, protocolo industrial sem autenticação	Disrupção de processo físico, comprometimento de OT	Firmware analysis, scan Claroty/Nozomi	OT Security / Infra

CVSS v4.0 em Profundidade

O CVSS (Common Vulnerability Scoring System), mantido pelo FIRST, é um padrão de medição de severidade técnica — não de risco de negócio. A versão 4.0 introduz quatro grupos de métricas e elimina a métrica Scope, tornando o modelo mais preciso para ambientes modernos.

Os Quatro Grupos de Métricas do CVSS v4.0

Base (CVSS-B)

Características intrínsecas da vulnerabilidade. Não muda com o tempo nem com o ambiente. Componentes: Attack Vector (AV), Attack Complexity (AC), Attack Requirements (AT), Privileges Required (PR), User Interaction (UI) e impactos em Confidentiality (VC/SC), Integrity (VI/SI) e Availability (VA/SA).

Threat (CVSS-BT)

Ajusta o score base pela maturidade do exploit. Valores: Not Defined, Unreported, Proof-of-Concept, Attacked. Um CVE com exploit público e uso ativo recebe penalidade máxima. Equivalente ao antigo Temporal do CVSS v3.

Environmental (CVSS-BE / BTE)

Ajusta para o contexto do seu ambiente: Modified Attack Vector, valor real dos ativos afetados (Confidentiality/Integrity/Availability Requirement). Um servidor de backup tem CR diferente de um sistema de pagamento.

Supplemental

Métricas adicionais informativas: Safety, Automatable, Recovery, Value Density, Vulnerability Response Effort, Provider Urgency. Não afetam o score final; auxiliam na comunicação e triagem.

Exemplo de Vetor CVSS v4.0 e Interpretação

`CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N`

- **AV:N** — Attack Vector: Network. Explorável remotamente pela rede.
- **AC:L** — Attack Complexity: Low. Não requer condições especiais.
- **AT:N** — Attack Requirements: None. Sem pré-requisitos adicionais.
- **PR:N** — Privileges Required: None. Sem autenticação necessária.
- **UI:N** — User Interaction: None. Automático, sem interação humana.
- **VC:H/VI:H/VA:H** — Impacto total em C/I/A no componente vulnerável.

Este vetor hipotético representaria uma falha crítica explorada remotamente, sem autenticação, com impacto total. O score base seria próximo do máximo.

⚠ CVSS mede severidade técnica. Um CVSS 9,8 em ativo isolado, sem exploit e sem dado sensível pode ser P2. Um CVSS 5,3 em API pública com exploit ativo pode ser P0. O score nunca deve ser usado isoladamente para priorizar.

EPSS, KEV e Inteligência de Exploração

Nenhum dos três — CVSS, EPSS e KEV — é substituto dos outros. Cada um responde a uma pergunta diferente. Usá-los em conjunto, com pesos e governança, é o que diferencia priorização baseada em evidência de triagem por número.

Sinal	O que responde	O que NÃO responde	Fonte / Metodologia	Frequência de Update
CVSS Base	Qual é a severidade técnica intrínseca da vulnerabilidade?	Se será explorada. Qual o contexto do meu ambiente. Impacto de negócio.	FIRST. Score calculado por fórmula a partir de métricas do vetor.	Quando o CVE é publicado ou revisado.
EPSS	Qual a probabilidade estimada de exploração nos próximos 30 dias?	Se o seu ativo específico será atacado. Impacto pós-exploração. Evidência de exploração passada.	FIRST. Modelo de ML treinado em dados de exploração observados (telemetria, threat feeds).	Diariamente. Score flutua.
CISA KEV	Esta vulnerabilidade tem exploração ativa conhecida, confirmada pela CISA?	Probabilidade futura. Escopo de impacto. Se o seu ativo é alvo.	CISA. Curadoria manual de vulnerabilidades com exploit confirmado em uso.	Contínuo. CVEs adicionados conforme confirmação de exploração.
Exploit Público	Existe código de exploração disponível publicamente (PoC/Metasploit/ExploitDB)?	Se o exploit é confiável, se requer modificação, impacto real.	NVD, CVSS Threat, ExploitDB, GitHub, threat feeds.	Variável. Pode aparecer dias/semanas após CVE.

Como Combinar os Sinais com Governança

1

KEV Confirmado

Override automático para P0. Exploração ativa é evidência concreta, independente do CVSS score.

2

EPSS Alto (≥ 0,5)

Elevar prioridade em 1 nível. EPSS alto indica alta probabilidade de exploração futura no horizonte de 30 dias (estimativa do modelo — não certeza).

3

Exploit Público Confirmado

Elevar prioridade. Reduz barrier to entry para o atacante. Combinado com exposição, torna-se gatilho de urgência.

4

CVSS + Contexto

Score base ajustado por Environmental e Threat. Sempre contextualizar com exposição, BIA e reachability antes de definir prioridade final.

Fonte: FIRST EPSS (https://www.first.org/epss) e CISA KEV Catalog (https://www.cisa.gov/known-exploited-vulnerabilities-catalog). Scores e limiares apresentados são referências metodológicas, não certificações de exploração de CVEs específicos.

Exposição e Reachability: Onde o Ativo Está no Mapa de Ataque

Exposição descreve a posição do ativo em relação ao attacker. Reachability descreve se o caminho entre o attacker e o alvo final (dado, processo, identidade) é tecnicamente viável. Um ativo pode estar exposto na internet e ter reachability zero para dados críticos — ou estar isolado internamente com reachability direta via lateral movement.

Espectro de Exposição

Nível	Descrição	Multiplicador de Risco
Internet-facing direto	IP público, sem proxy, sem WAF	Máximo
Publicado via LB/WAF	Internet com controle intermediário	Alto (controle pode falhar ou ser bypassado)
Acessível via VPN	Requer autenticação de rede	Moderado
Rota interna / lateral	Acessível após comprometimento inicial	Moderado-alto se Crown Jewel
Segmento restrito	Microsegmentação, allow-list de origem	Baixo-moderado
Air-gapped	Sem conectividade de rede	Muito baixo
Sem rota ativa	Interface presente mas sem rota configurada	Baixo (monitorar drift)

Diagrama de Caminho de Ataque

Reachability de Dados e Identidade

- **Reachability de rede:** existe rota TCP/IP entre attacker e ativo vulnerável?
- **Reachability de dados:** após exploração, o attacker alcança dados sensíveis, processos críticos ou identidades privilegiadas?
- **Reachability de identidade:** a identidade comprometida tem permissões que permitem escalar para outros sistemas?

BIA — Business Impact Analysis na Gestão de Vulnerabilidades

O BIA transforma "servidor importante" em impacto mensurável. Sem ele, toda a cadeia de priorização fica ancorada em severidade técnica sem contexto de negócio. O BIA deve ser mantido atualizado — um BIA de 18 meses descreve uma empresa que pode não existir mais operacionalmente.

Dimensões do Impacto no BIA

- **Financeiro:** receita em risco por hora de indisponibilidade, multas contratuais, penalidades regulatórias (LGPD, PCI DSS, SOX).
- **Operacional:** processos de negócio paralisados, SLA de atendimento comprometido, cadeia de suprimentos afetada.
- **Regulatório:** obrigações de notificação (ANPD), reportes mandatórios, impacto em certificações (ISO 27001, SOC 2).
- **Reputacional:** exposição pública de dados, notícias negativas, perda de confiança de clientes e parceiros.
- **Segurança da Informação:** comprometimento de confidencialidade, integridade ou disponibilidade de dados críticos.

Parâmetros Temporais do BIA

Parâmetro	Definição	Aplicação em VM
RTO	Recovery Time Objective: tempo máximo para restaurar serviço após incidente.	Define urgência de remediação de falhas que causam indisponibilidade.
RPO	Recovery Point Objective: perda máxima tolerável de dados.	Orienta criticidade de falhas que afetam integridade ou disponibilidade de dados.
MTPD / MAO	Maximum Tolerable Period of Disruption: ponto de ruptura do negócio.	Falhas em sistemas com MTPD < 4h devem ser tratadas como críticas.
Criticidade BIA	Nível classificatório: Crítico / Importante / Não Crítico.	Multiplicador direto no score de priorização e na definição de SLA.

Dependências e Crown Jewels

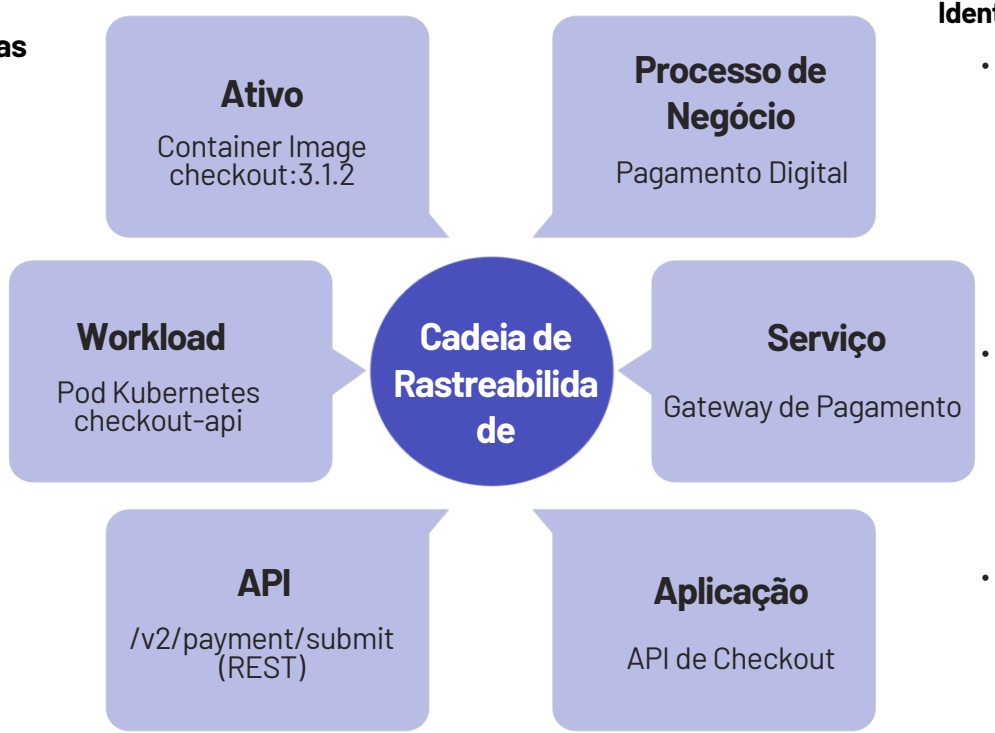
O BIA deve mapear dependências diretas e indiretas entre processos e ativos. Um ativo de suporte (ex.: serviço de autenticação, HSM, API gateway) pode ter BIA crítico por herança — se ele cair, processos críticos param mesmo sem relação direta.

Cadeia de Rastreabilidade BIA: Do Processo ao Finding

A cadeia de rastreabilidade conecta cada finding técnico ao processo de negócio que ele pode afetar. Esta ligação é o que torna um relatório de vulnerabilidade interpretável por um CTO, CFO ou conselho — e é o que transforma dados técnicos em decisão de negócio documentável.

Dependências Diretas e Indiretas

- **Diretas:** o ativo vulnerável está na cadeia de execução do processo crítico. Ex.: banco de dados de pedidos.
- **Indiretas:** o ativo vulnerável suporta uma dependência do processo. Ex.: serviço de autenticação usado pelo gateway de pagamento. Uma falha aqui paralisa pagamentos sem atacar o gateway diretamente.
- **Transitivas:** biblioteca de criptografia usada por 12 serviços diferentes; um único finding afeta múltiplos processos de negócio com BIAs distintos.



Identificando Crown Jewels via Cadeia

- Crown jewels são ativos cuja comprometimento causa impacto máximo ao negócio. São identificados percorrendo a cadeia de trás para frente: quais ativos, se comprometidos, afetam processos com MTPD < 4h, impacto financeiro > threshold ou notificação regulatória obrigatória?
- **Exemplos típicos:** HSM de chaves de pagamento, banco de dados de clientes com dados financeiros, IdP/SSO (Identity Provider), pipeline de CI/CD com acesso a produção, sistema de faturamento e ERP.
- **Nota operacional:** a cadeia precisa ser mantida atualizada. Ambientes cloud mudam rapidamente — um novo serviço pode se tornar um Crown Jewel sem que o BIA seja atualizado.

Inventário e Enriquecimento Técnico: Modelo de Dados

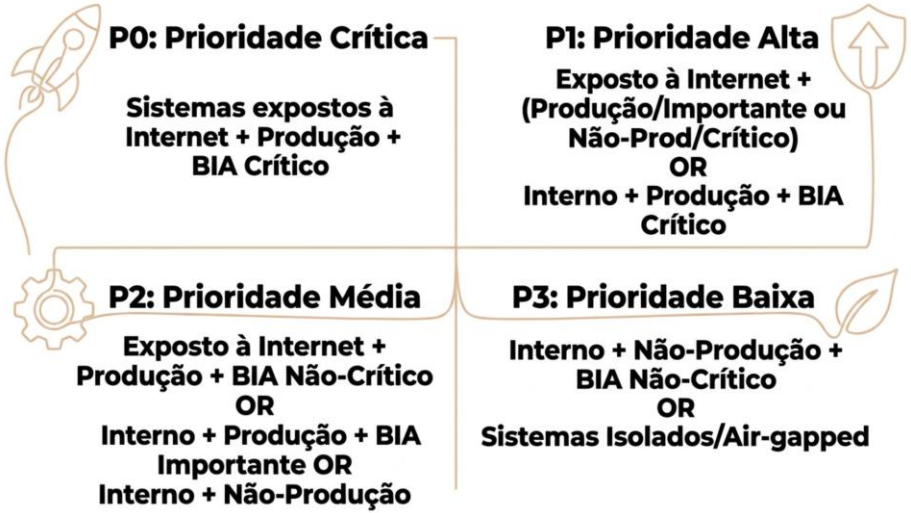
Um finding sem contexto de ativo é ruído. O modelo de dados do inventário é a fundação de toda priorização baseada em evidência. Campos ausentes não são neutros — representam risco não mensurado. A governança de campos obrigatórios deve ser um KPI do programa de VM.

Campo	Tipo	Obrigatório?	Fonte / Nota
asset_id	String único	**Sim**	CMDB / Inventário cloud. Âncora de todos os findings.
owner_tecnico	Equipe / pessoa	**Sim**	CMDB. Sem owner, o SLA não tem responsável.
business_owner	Nome / área	**Sim**	Necessário para aceite de risco e BIA.
ambiente	prod / staging / dev / test	**Sim**	Impacta prioridade diretamente. Governa SLA.
criticidade_bia	crítico / importante / não crítico	**Sim**	Output do BIA. Exige revisão periódica.
internet_facing	boolean	**Sim**	Define multiplicador de exposição. Validar com ASM.
dados_sensiveis	PII / PCI / PHI / nenhum	**Sim**	Impacta obrigações regulatórias pós-exploit.
identidade_associada	service account, role IAM	Recomendado	Identifica escalada de privilégio potencial.
eol	boolean + data	Recomendado	EOL = sem patch disponível; exige plano de substituição.
patch_window	schedule / ad-hoc / restrito	Recomendado	Informa viabilidade de remediação no SLA.
controles_compensatorios	WAF / EDR / segmentação / nenhum	Recomendado	Reduz score de risco residual se ativo e testado.
ultima_evidencia	timestamp	**Sim**	Evidência desatualizada (> 30 dias) = incerteza de estado.
data_descoberta	timestamp	**Sim**	Base para cálculo de MTTR e tempo de exposição.
cloud_account / regiao	string	Cloud only	Necessário para correlação com CSPM e inventário cloud.

⚠ Campos ausentes não devem ser assumidos como favoráveis. Um internet_facing desconhecido deve ser tratado como *true* para fins de priorização conservadora, até confirmação.

Matriz Principal de Categorização e Prioridade

A matriz cruza três dimensões objetivas — Exposição, Ambiente e Criticidade BIA — para produzir uma prioridade padrão P0–P3. Overrides manuais documentados permitem elevar ou reduzir a prioridade quando a evidência técnica justificar.



Overrides e Exceções Documentadas

Condição	Override para
Ransomware TTPs confirmados no setor	P0 imediato, independente de BIA
Acesso inicial (Initial Access) sem autenticação	Elevar 1 nível
Identidade privilegiada (admin, root, cloud admin)	Elevar 1 nível
Dados regulados (PII, PCI, PHI) acessíveis	Elevar 1 nível
Ativo sem patch disponível (EOL/vendor)	Escalar para aceite de risco + mitigação compensatória
Controle compensatório ativo e testado	Pode reduzir 1 nível com evidência documentada

Regra P0 — Critérios de Gatilho

Um finding é **P0** quando atender a qualquer uma das condições abaixo:

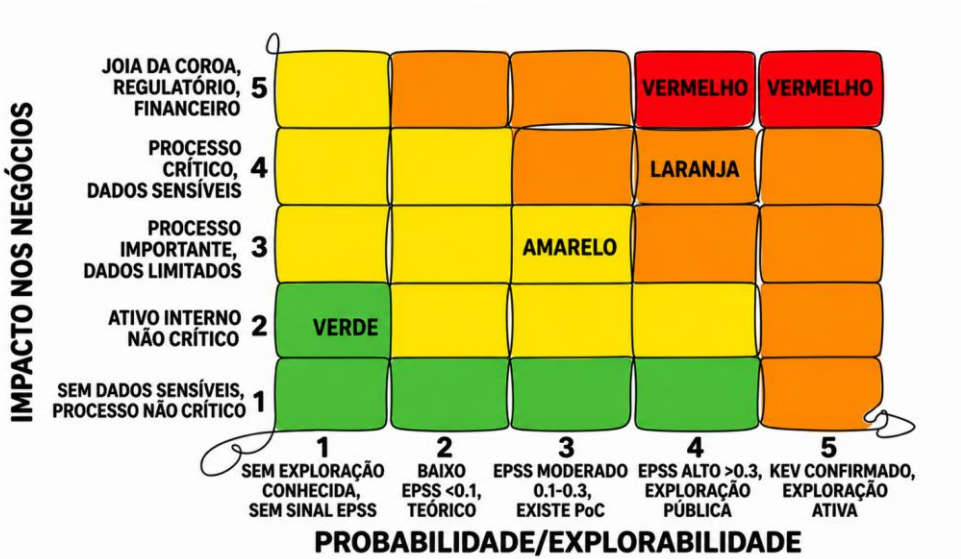
- Consta no CISA KEV (exploração ativa confirmada) **E** ativo em produção ou internet-facing.
- Combinação: internet-facing **+** produção **+** BIA crítico **+** caminho de ataque plausível identificado.
- RCE sem autenticação em qualquer ativo de produção com dados sensíveis.
- Segredo exposto com acesso imediato a sistema ou dado crítico.
- Comprometimento confirmado de supply chain em pipeline ativo.

Matriz 5×5 de Risco: Ferramenta de Decisão e Comunicação

A matriz 5×5 de risco é uma ferramenta visual para comunicação com stakeholders e para documentar decisões de priorização. Ela não substitui evidência técnica — é complementar à matriz P0–P3 e aos modelos quantitativos. Seus eixos devem ter critérios objetivos para evitar subjetividade.

Critérios Objetivos por Eixo

Nível	Probabilidade / Explorabilidade	
1	Sem exploit, sem EPSS relevante, vetor local, requer autenticação forte	Ativo não crítico, sem dados sensíveis, sem processo dependente
2	EPSS < 0,10, exploit teórico, requer condições especiais	Processo interno não crítico, dados não classificados
3	EPSS 0,10–0,30, PoC público, exploit com complexidade moderada	Processo importante, dados sensíveis com escopo limitado
4	EPSS > 0,30, exploit público e funcional, internet-facing	Processo crítico, dados PII/PCI, MTPD < 8h
5	KEV confirmado, exploração ativa observada, wormable ou automatable	Crown jewel, impacto financeiro imediato, notificação regulatória obrigatória



Zonas de Risco e Ação

Baixo (1–4)
Monitorar. Correção no ciclo regular, P3. Sem urgência operacional.

Moderado (5–9)
Planejar correção. P2–P3. Controle compensatório se necessário.

Alto (10–16)
Prioridade elevada. P1. SLA de 7 dias. Mitigação imediata se sem patch.

Crítico/Imediato (≥ 17)
P0. Ação em horas/24h. Escalar para CISO. Registrar evidência e decisão.

A matriz é uma ferramenta de comunicação. Decisões finais devem ser baseadas em evidência técnica, não apenas no quadrante. Registre as premissas de cada posicionamento.

Modelo Quantitativo A — Score Ponderado

O modelo de score ponderado normaliza múltiplos fatores em uma escala única (0–100) e aplica pesos calibrados para produzir uma fila ordenada de remediação. **Os pesos e scores apresentados são didáticos** — cada organização deve calibrar conforme seu perfil de risco, setor e apetite.

Fórmula Principal

$$Score = 0{,}25 \times S + 0{,}25 \times E + 0{,}20 \times Ex + 0{,}20 \times I_{BIA} + 0{,}10 \times F_A$$

Onde:

- **S** = Severidade (CVSS normalizado 0–100)
- **E** = Exploitabilidade (EPSS × 100 + sinal de exploit público)
- **Ex** = Exposição (score de posição no espectro de exposição)
- **I_BIA** = Impacto BIA (score de criticidade de negócio)
- **F_A** = Fragilidade do Ativo (EOL, sem controle compensatório, patch window restrito)

Tabela de Pontuação por Fator (Didática)

Fator	Critério	Score (0–100)
Severidade	CVSS 9–10 / 7–8,9 / 4–6,9 / < 4	90–100 / 60–89 / 30–59 / 0–29
Exploitabilidade	KEV / Exploit+EPSS alto / EPSS mod / Sem exploit	100 / 70–90 / 40–69 / 0–39
Exposição	Internet direto / LB+WAF / VPN / Interno / Isolado	100 / 75 / 50 / 30 / 5
Impacto BIA	Crítico / Importante / Não crítico	100 / 60 / 20
Fragilidade	EOL sem patch / Sem controle / Controle parcial / Controle ativo	100 / 70 / 40 / 10

Faixas de Prioridade

P0 — Score ≥ 80
Remediação em 24h. Escalar imediatamente.

P1 — Score 60–79
Remediação em 7 dias. Monitoramento diário.

P2 — Score 40–59
Remediação em 30 dias. Plano documentado.

P3 — Score < 40
Remediação em 90 dias ou aceite de risco.

⚠ Cuidado com dupla contagem: CVSS já inclui componentes de exploitabilidade no Base Score. Evitar usar CVSS Exploitability sub-score e EPSS como fatores independentes sem normalização — isso infla artificialmente o score de exploração.

Modelo Quantitativo B — Combinação Tóxica (Multiplicativo)

O modelo multiplicativo representa o conceito de "combinação tóxica" — quando múltiplos fatores de risco coexistem, o risco resultante não é aditivo, é amplificado. Uma falha de severidade moderada com exploit ativo, em ativo internet-facing, com dados regulados e sem controle compensatório resulta em risco desproporcional ao CVSS isolado.

Fórmula Multiplicativa

$$Risco = CVSS_{norm} \times Expl \times Exp \times I_{BIA} \times F_C$$

Onde:

- **CVSS_norm** = CVSS/10 → escala 0,0–1,0
- **Expl** = Exploitabilidade: KEV=1,0 / Exploit+EPSS alto=0,8 / EPSS mod=0,5 / Sem exploit=0,2
- **Exp** = Exposição: Internet direto=1,0 / LB=0,8 / VPN=0,5 / Interno=0,3 / Isolado=0,05
- **I_BIA** = Impacto: Crítico=1,0 / Importante=0,6 / Não crítico=0,2
- **F_C** = Fator de controle: Sem controle=1,0 / Parcial=0,6 / Controle ativo=0,3

Resultado máximo: 1,0 × 1,0 × 1,0 × 1,0 × 1,0 = 1,0 (normalizado para 100).

Resultado mínimo: 0,1 × 0,2 × 0,05 × 0,2 × 0,3 ≈ 0,00006.

Por que o Modelo Multiplicativo Amplifica Combinações Críticas

Considere dois exemplos didáticos:

Cenário	CVSS_norm	Expl	Exp	I_BIA	F_C	Risco
CVSS 9,8, isolado, sem exploit, BIA baixo, controle ativo	0,98	0,2	0,05	0,2	0,3	**0,0006**
CVSS 6,5, internet-facing, KEV, BIA crítico, sem controle	0,65	1,0	1,0	1,0	1,0	**0,65**

O CVSS 9,8 isolado resulta em risco contextual ~0,06% do máximo. O CVSS 6,5 com combinação tóxica resulta em risco 65% do máximo — mais de 1.000× superior.

Governança do Modelo Multiplicativo

- Registrar premissas e multiplicadores utilizados em cada cálculo.
- Revisão humana obrigatória para scores acima de 0,5 (P0/P1).
- Calibrar multiplicadores periodicamente contra dados históricos de exploração real no ambiente.
- Não usar o modelo como decisão automática — é ferramenta de suporte à decisão.

Exemplo Calculado 1 — Gateway de Pagamento em Produção

Natureza do exemplo: Este é um cenário didático construído para ilustrar a aplicação dos dois modelos. Scores e multiplicadores são calculados com os critérios definidos nesta apresentação, não representam CVEs reais em exploração.

Entradas do Cenário

Atributo	Valor
Ativo	Gateway de pagamento — produção
Ambiente	Produção
Internet-facing	Sim (exposto via LB com WAF)
Criticidade BIA	Crítico (MTPD = 2h, impacto financeiro direto)
Dados	PCI DSS — dados financeiros de clientes
Identidade associada	Service account com permissão limitada
CVSS Base	6,5 (vetor: Network, AC: Low, PR: Low)
EPSS	Alto (> 0,50 — probabilidade estimada pelo modelo)
Exploit público	Sim — PoC disponível em repositório público
KEV CISA	Sim — consta no catálogo
Controle compensatório	WAF ativo com regra parcial para o vetor

Cálculo e Decisão

Modelo	Cálculo	Score
Ponderado (A)	0,25×65 + 0,25×95 + 0,20×75 + 0,20×100 + 0,10×40	**79,5 → P0/P1**
Multiplicativo (B)	0,65 × 1,0 × 0,8 × 1,0 × 0,6	**0,312 → P0 (KEV override)**

Decisão Final: P0

Override KEV

Presença no CISA KEV aciona P0 automaticamente. EPSS alto e exploit público reforçam a decisão.

Ação Imediata

Validar cobertura da regra WAF. Isolar serviço se patch não disponível em 4h. Aplicar patch/rebuild em janela emergencial.

Owner e Evidência

Owner: equipe de Infra + AppSec. Evidência: reteste com scanner autenticado pós-patch, log de change, ticket de aprovação emergencial.

Exemplo Calculado 2 — CVSS 9,8 em Ambiente de Teste Isolado

Objetivo deste exemplo: demonstrar que severidade técnica alta não implica prioridade alta quando o contexto operacional reduz substancialmente a probabilidade e o impacto. Este é o cenário mais comum de desperdício de esforço de remediação.

Entradas do Cenário

Atributo	Valor
Ativo	Servidor de testes de integração
Ambiente	Teste — isolado, sem rota para produção
Internet-facing	Não
Criticidade BIA	Não crítico (sem dados reais, sem processo de negócio dependente)
Dados	Dados sintéticos de teste, sem PII ou PCI
CVSS Base	9,8 (RCE, network, sem autenticação)
EPSS	Baixo (< 0,05) — sem sinal de exploração ativa no modelo
Exploit público	Não confirmado no horizonte atual
KEV CISA	Não consta
Rota para produção	Inexistente — segmento isolado por firewall dedicado
Owner	Definido — equipe de QA

Cálculo e Decisão

Modelo	Cálculo	Score
Ponderado (A)	0,25×98 + 0,25×15 + 0,20×5 + 0,20×20 + 0,10×30	**35,75 → P3**
Multiplicativo (B)	0,98 × 0,2 × 0,05 × 0,2 × 1,0	**0,00196 → P3**

Decisão Final: P2/P3

Por que não é P0

CVSS alto mede severidade intrínseca da falha, não risco contextual. Sem exposição, sem exploit ativo, sem dados reais e sem BIA — os fatores de risco são mínimos.

Ação Recomendada

Correção planejada no próximo ciclo de atualização do ambiente de teste. Considerar desativação do componente se não utilizado. Verificar se o ambiente pode tornar-se internet-facing no futuro.

Monitoramento

Reavaliar se: EPSS aumentar significativamente, exploit público confirmar-se, ou rota para produção for criada. Qualquer mudança de contexto requalifica a prioridade.

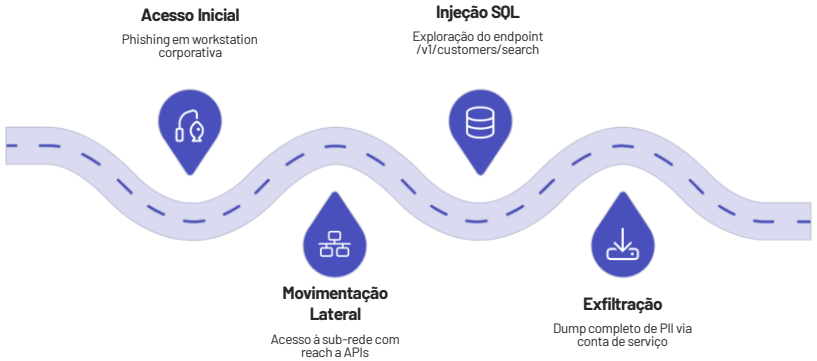
Exemplo Calculado 3 — API Interna com Dados Pessoais e Identidade Privilegiada

Este exemplo demonstra que um ativo interno pode ser P0 quando a combinação de reachability lateral, dados regulados e identidade privilegiada cria um caminho de ataque viável de alta consequência. Exposição interna não significa risco baixo.

Entradas do Cenário

Atributo	
Ativo	API interna de consulta de clientes — produção
Internet-facing	Não (acessível apenas na rede corporativa)
Criticidade BIA	Crítico — base de dados de PII LGPD, 3M de registros
CVSS Base	8,1 (SQL Injection, Network, AC: Low, PR: Low)
EPSS	Moderado (0,15–0,30)
Identidade associada	Service account com leitura total em todos os schemas do banco
Reachability lateral	Acessível a partir de qualquer estação da rede corporativa comprometida
Controle de rede	Firewall interno com regra parcial (permite acesso de subnets amplas)
Dados	PII LGPD — nome, CPF, endereço, histórico de compras

Análise de Caminho de Ataque e Cálculo



Modelo	Cálculo	Score
Ponderado (A)	0,25×81 + 0,25×55 + 0,20×30 + 0,20×100 + 0,10×70	**67,75 → P1**
Multiplicativo (B)	0,81 × 0,5 × 0,3 × 1,0 × 0,6	**0,0729 → P1**

Override para P0: dados PII LGPD com 3M+ registros e notificação obrigatória à ANPD aciona override regulatório, elevando para P0.

Ações: Caminho de Ataque, Redução de Privilégio e Segmentação

- Reduzir permissão da service account ao mínimo necessário (principle of least privilege).
- Aplicar microsegmentação — restringir acesso à API apenas a subnets autorizadas.
- Aplicar WAF com regra de SQL Injection no proxy interno da API.
- Corrigir a falha de injeção no código (correção definitiva).
- Ativar logging de todas as queries com alertas de volume anômalo no SIEM.

Remediação e Mitigação Quando o Patch Não É Possível

Nem toda vulnerabilidade pode ser corrigida com um patch. EOL, dependência de vendor, janela de manutenção indisponível ou ausência de patch oficial exigem controles compensatórios. **Mitigação não elimina a vulnerabilidade** — reduz a probabilidade ou o impacto e exige prazo de revisão e evidência de eficácia.

Controle Compensatório	Quando Usar	Limitação	Risco Residual	Teste de Eficácia
Virtual Patching (WAF/IPS/NGFW)	Falha de injeção, RCE via HTTP, vetor de rede sem patch disponível	Bypass via encoding, novo vetor, regra desatualizada	Moderado — attacker pode adaptar payload	Teste de PoC após ativação da regra; revisar mensalmente
Bloqueio de Rota/Porta	Serviço desnecessariamente exposto, vetor de rede específico	Pode quebrar funcionalidade; não endereça vetores alternativos	Baixo se rota única; alto se lateral movement possível	
Microsegmentação	Ativo crítico acessível de subnets amplas, reachability lateral	Implementação complexa; risco de bloqueio de tráfego legítimo	Reduz significativamente a superfície de ataque lateral	Validar rotas bloqueadas com scan de reachability
Desativação de Função/Feature	Feature vulnerável não utilizada (ex.: XMLRPC, SNMP v1)	Pode afetar integrações legadas; verificar dependências	Baixo se função não for reativada	Confirmar via scan que feature não responde mais
MFA e Redução de Privilégio	Falhas de autenticação, escalada de privilégio, identidade comprometida	Não corrige a falha técnica; usuário pode ser phishado mesmo com MFA	Moderado — reduz impacto de comprometimento de credencial	Teste de bypass de autenticação pós-implementação
Isolamento / Quarentena	Ativo crítico sem patch, alto risco, sem alternativa imediata	Impacto operacional significativo; solução temporária	Baixo enquanto isolado — monitorar tentativas de acesso	Confirmar isolamento via scan de reachability
Rotação de Segredos	Segredo exposto em repositório, variável ou log	Segredo antigo pode estar cacheado; revogar em todos os pontos	Muito baixo se rotação completa e confirmada	Verificar que chave antiga não autentica mais
Monitoramento SIEM/IDS	Sempre — especialmente quando patch ou mitigação não é possível	Detecção, não prevenção; depende de assinatura atualizada	Alto — vulnerabilidade permanece; risco é de detecção tardia	Testar alertas com tráfego simulado do exploit

⊗ Mitigação sem prazo de revisão se torna risco residual permanente. Todo controle compensatório deve ter: data de implementação, responsável, data de revisão obrigatória e critério de encerramento (patch disponível, ativo desativado ou aceite formal de risco).

Workflow Operacional, SLA, Exceção e Evidência

O processo operacional é onde a priorização se torna ação. Sem workflow definido, SLA documentado e evidência de fechamento, o programa de VM não é auditável e não demonstra maturidade para fins de GRC e conformidade.

Aceite Formal de Risco e Critérios de Reabertura

- **Aceite de risco** é uma decisão documentada, não omissão. Deve conter: justificativa técnica, controles compensatórios ativos, risk owner identificado, data de validade (máximo 90 dias para P1, 180 dias para P2) e critérios de reabertura.
- **Critérios de reabertura:** EPSS aumentar significativamente; CVE entrar no CISA KEV; exploit público confirmado; mudança no ambiente do ativo (novo dado, nova exposição); controle compensatório falhar ou expirar.
- **Compensating Control:** deve ser registrado com evidência de teste de eficácia, não apenas declarado. WAF sem teste de cobertura não é controle compensatório válido para auditoria.
- **Change Management:** P0 pode exigir change emergencial — documentar aprovação, impacto, rollback e resultado. P1/P2 seguem processo padrão com janela planejada.

Tabela de SLA por Prioridade (Didática — Adaptar ao Setor)

Prioridade	SLA de Remediação	SLA de Mitigação Inic	Escalação
P0	24 horas	4 horas (controle compensatório)	CISO + CTO imediato
P1	7 dias corridos	24 horas	Manager + Security Lead
P2	30 dias corridos	72 horas se controle disponível	Team Lead
P3	90 dias corridos	Opcional — avaliar custo-benefício	Revisão trimestral

Métricas, Dashboard e Síntese

Métricas Essenciais do Programa de VM

MTTR

Mean Time to Remediate

Por prioridade (P0/P1/P2/P3). Tendência de melhora ou piora ao longo do tempo.

SLA%

KEV dentro do SLA

% de vulnerabilidades do CISA KEV remediadas dentro do SLA P0. Indicador regulatório.

BIA

Backlog Ponderado

Total de findings abertos × peso de criticidade BIA. Indica risco acumulado real, não apenas volume.

Owner

% sem Owner

Findings sem responsável definido. Qualquer valor > 0% indica falha de CMDB ou processo.

Métricas Complementares

- **Tempo de exposição por prioridade:** dias entre data_descoberta e data_encerramento. Indica velocidade real de resposta.
- **Taxa de recorrência:** % de findings reabertos após encerramento. Indica qualidade da remediação.
- **Cobertura de inventário:** % de ativos com última evidência de scan ≤ 30 dias.
- **Eficácia de mitigação:** % de controles compensatórios com teste de eficácia documentado.
- **Risco residual acumulado:** soma ponderada dos scores de findings em aceite de risco ativo.
- **Qualidade da evidência:** % de fechamentos com evidência técnica válida (scan pós-fix, log de patch).

Síntese: O que É Priorização Baseada em Risco

Priorizar não é ordenar por CVSS. É combinar severidade técnica, probabilidade de exploração, reachability, criticidade de negócio e capacidade de recuperação — documentando cada decisão com evidência.

Severidade + Exploração

CVSS contextualizado por EPSS, KEV e exploit público. Nenhum score isolado é suficiente.

Exposição + Caminho

Reachability de rede, dados e identidade. Um ativo isolado tem risco diferente de um internet-facing mesmo com mesmo CVE.

BIA + Recuperação

Criticidade de negócio determina impacto pós-exploração. RTO/RPO determinam urgência de restauração.

Referências Consultadas

- **NIST SP 800-40 Rev. 4** — Guide to Enterprise Patch Management Planning. *csrc.nist.gov/pubs/sp/800/40/r4/final*
- **CISA KEV Catalog** — Known Exploited Vulnerabilities. *cisa.gov/known-exploited-vulnerabilities-catalog*
- **FIRST CVSS v4.0** — Common Vulnerability Scoring System. *first.org/cvss*
- **FIRST EPSS** — Exploit Prediction Scoring System. *first.org/epss*
- **VM Chaining Framework** — Vulnerability Management Chaining (referência acadêmica). *arxiv.org/html/2506.01220v2*

Scores e multiplicadores dos exemplos calculados são didáticos. Não afirmam exploração ativa de CVEs específicos. BIA e CMDB exigem atualização periódica para manter a priorização válida. Sempre distinguir orientação oficial (NIST, CISA, FIRST) de prática operacional e exemplo didático.

“Se você trabalha com gestão de vulnerabilidades, uma boa prática é começar pequeno: escolha um conjunto de ativos críticos, conecte esses ativos ao BIA, adicione exposição e evidência de exploração e construa uma fila priorizada.
Depois, evolua o processo com automação, métricas e revisão periódica.
A maturidade não está em ter mais alertas.
Está em tomar decisões melhores com as informações disponíveis.”

OBRIGADO !