CYVORA
CYBERSECURITY & AI DEFENSE

MODELO PÚBLICO DE DEMONSTRAÇÃO

Relatório de Avaliação de Segurança

Empresa Logística

Cenário fictício · 2.400 colaboradores · 14 centros de distribuição



LEITURA EXECUTIVA

Uma avaliação que conecta risco técnico, impacto no negócio e um plano claro de remediação.

100
vulnerabilidades confirmadas

4
riscos críticos priorizados

90 dias
plano de ação estruturado

Período da avaliação simulada
13 de outubro a 7 de novembro de 2026

Versão
1.0 · Final para diretoria

Empresa, números e achados são fictícios. Este documento demonstra a estrutura e o nível de profundidade de uma Avaliação de Segurança CYVORA.

01 · DECISÃO EM UMA PÁGINA

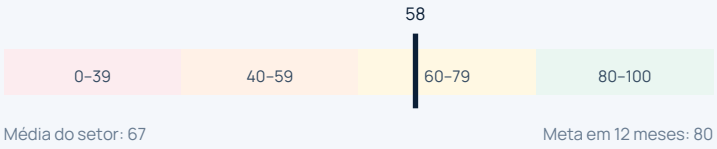
Risco alto, com um caminho objetivo para reduzi-lo.

No cenário simulado, um atacante externo conseguiria interromper a operação logística com ransomware em poucas horas; a recuperação levaria semanas.

ÍNDICE CYVORA DE POSTURA

58/100 · risco alto

112 controles avaliados



4
Riscos críticos
9 vulnerabilidades críticas

3h40
Até domínio do AD
No teste interno simulado

38%
VPN sem MFA
433 de 1.140 usuários

7 dias
Retenção de logs
Recomendado: 12 meses

TRÊS MENSAGENS PARA A DIRETORIA

01 — A porta de entrada está aberta.
A VPN tem uma falha explorada ativamente na internet, e 38% dos acessos remotos não exigem MFA.

02 — Os dados dos clientes estão expostos.
Uma falha na API permite consultar remessas, endereços e notas fiscais de outros clientes; se explorada, pode configurar incidente reportável à ANPD.

03 — O plano B não sobreviveria a um ataque.
Os backups do ERP ficam no mesmo domínio que o atacante dominaria, sem cópia imutável ou teste de restauração nos últimos 12 meses.

DECISÃO SOLICITADA

Aprovar o plano de 30 dias para tratar os quatro riscos críticos e elevar a nota estimada para 71/100.

02 · COMO A AVALIAÇÃO FOI CONDUZIDA

Cobertura ampla, evidências e supervisão especializada.

O cenário simula testes autorizados por escrito, janela acordada e validação dos achados com as equipes da organização.

Ficha do relatório	Configuração do cenário
Organização	Empresa fictícia do setor logístico · 2.400 colaboradores · 14 CDs
Tipo de avaliação	Postura de Segurança + Teste de Intrusão externo e interno
Período	13 de outubro a 7 de novembro de 2026 · 4 semanas
Equipe CYVORA	OFFENSIVE · CLOUD · GOVERNANCE
Referenciais	NIST CSF 2.0 · CIS Controls v8.1 · OWASP · ISO/IEC 27001:2022 · LGPD

248 ativos em seis superfícies

Superfície	Ativos no escopo	Tipo de teste
Perímetro e acesso remoto	31 IPs públicos, VPN, firewalls	Caixa-preta externo
Aplicações e APIs	Portal, app do motorista, 42 endpoints	Caixa-cinza · OWASP
Nuvem	3 contas AWS, tenant Microsoft 365	Revisão · CIS Benchmarks
Rede interna e identidade	AD, 2 data centers, 14 CDs	Intrusão a partir de estação padrão
Estações e servidores	120 estações e 38 servidores	Varredura autenticada + EDR
Pessoas e processos	1.140 usuários, 22 entrevistas, 64 documentos	Phishing simulado + análise documental

COMO TRABALHAMOS

01	02	03	04	05
Descoberta	Teste técnico	112 controles	IA supervisionada	Validação

Fora do escopo: sistemas de fornecedores, negação de serviço e engenharia social presencial.

03 · EXPOSIÇÃO TÉCNICA

A prioridade não é apenas corrigir. É corrigir na ordem certa.

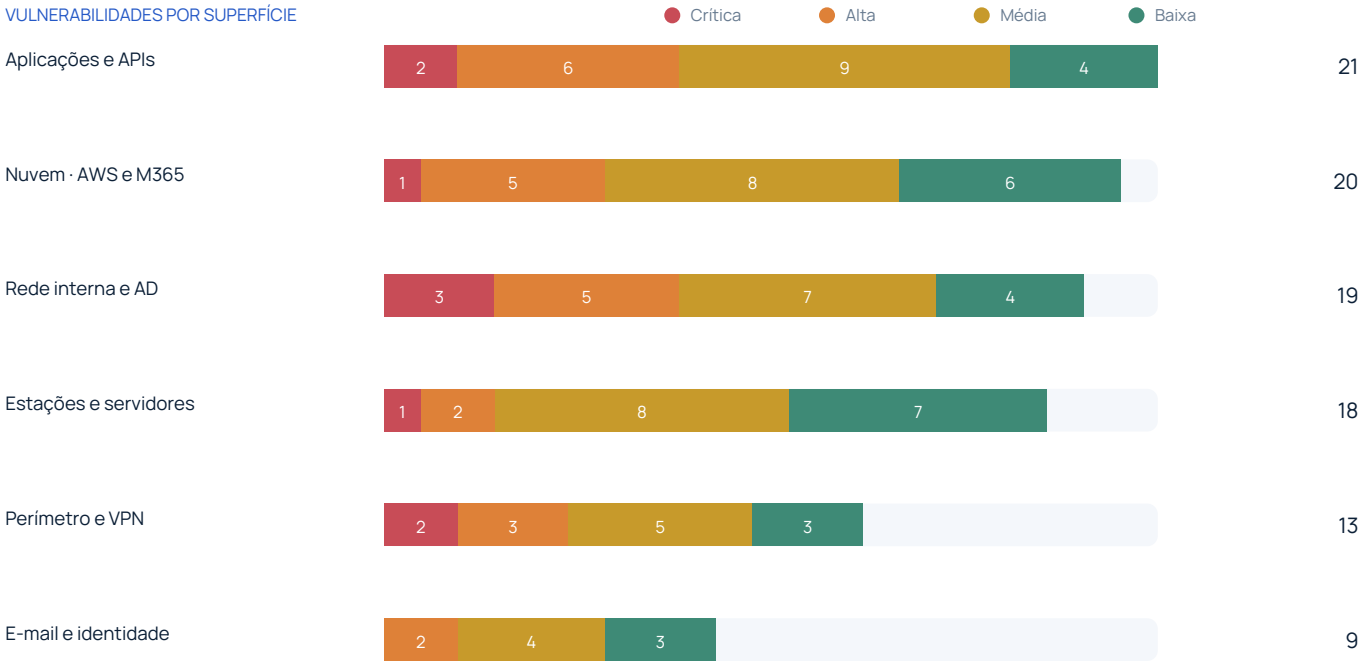
Foram confirmadas 100 vulnerabilidades no cenário; 61 tinham atualização publicada há mais de 90 dias.

100
Vulnerabilidades
Confirmadas, sem falsos positivos

9
Criticidade máxima
6 presentes no catálogo CISA KEV

61
Correções disponíveis
Atualização publicada há +90 dias

VULNERABILIDADES POR SUPERFÍCIE



POR QUE ISSO IMPORTA

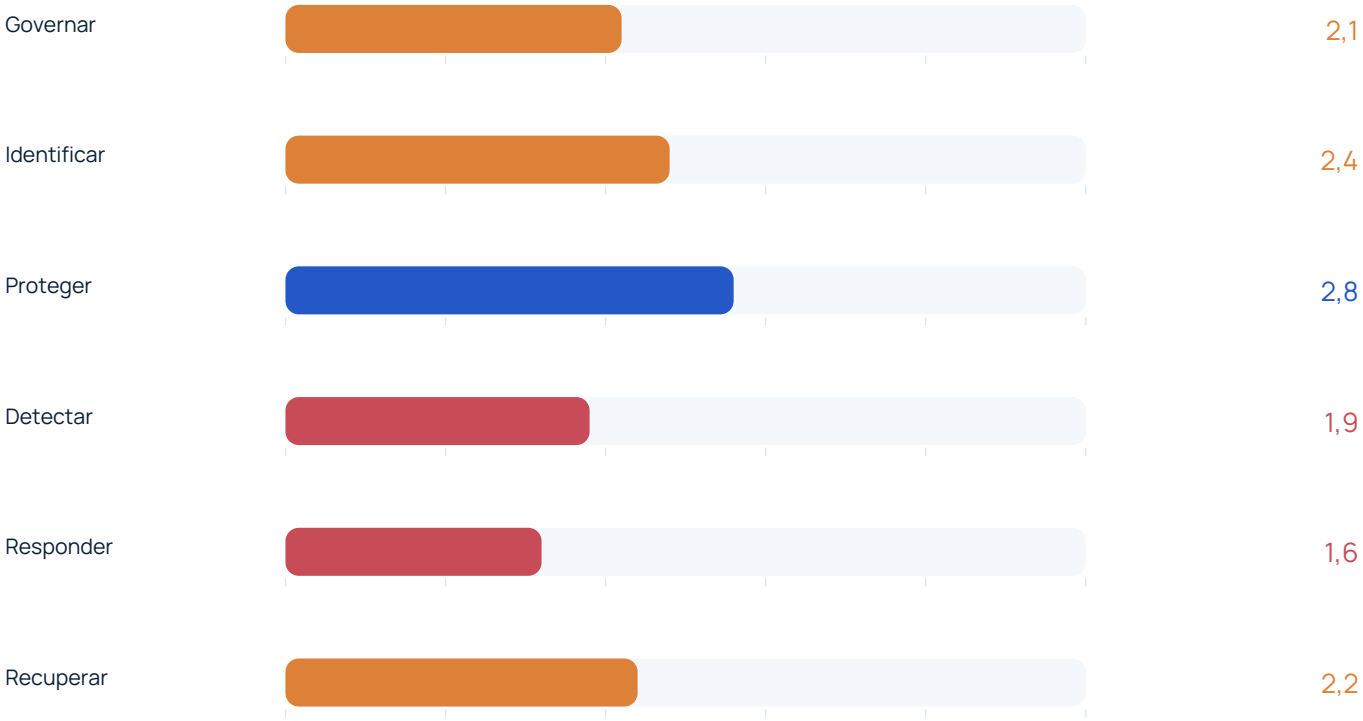
Rede interna e Active Directory concentram 3 das 9 vulnerabilidades críticas. Seis das nove críticas estão no catálogo de vulnerabilidades exploradas ativamente da CISA (KEV), elevando sua prioridade.

04 · CAPACIDADE DE DEFESA

Detectar e responder são os elos mais fracos.

A organização fictícia investiu em proteção, mas ainda não possui capacidade consistente para perceber e reagir a um ataque em andamento.

MATURIDADE MÉDIA POR FUNÇÃO · ESCALA DE 0 A 5



LEITURA EXECUTIVA

Resposta com maturidade 1,6 significa improviso nas primeiras 24 horas.

No cenário avaliado, não há plano testado, papéis definidos nem contato prévio com perícia e jurídico.

112 controles avaliados em entrevistas, evidências e testes · dados fictícios

05 · PROBABILIDADE × IMPACTO

Os quatro riscos críticos estão na zona vermelha.

Os 100 achados técnicos foram consolidados em 10 riscos de negócio, ordenados pela probabilidade de exploração e pelo impacto na operação.



C-01 9,8
VPN + MFA

C-02 9,1
API · BOLA

C-03 9,0
Backups

C-04 8,8
Conta de serviço

COMO LER A MATRIZ

A cor combina probabilidade e impacto: vermelho para 15 ou mais, laranja de 10 a 14, amarelo de 5 a 9 e verde abaixo de 5.

05 · PRINCIPAIS ACHADOS

Dez riscos de negócio, com severidade e impacto explícitos.

"Controle" indica ausência ou falha de controle avaliada pelo CIS Controls v8.1, e não uma vulnerabilidade com nota CVSS.

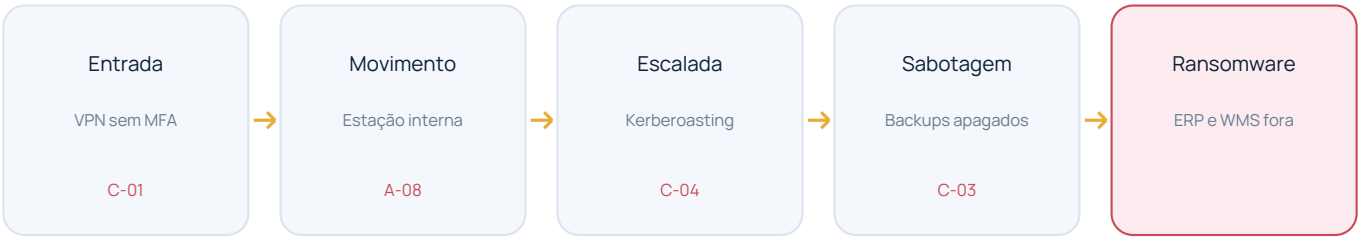
ID	Achado	Sev.	CVSS	Superfície	Impacto no negócio
C-01	VPN com falha explorada ativamente e 38% dos acessos sem MFA	Crítica	9,8	Perímetro	Entrada direta para ransomware
C-02	API do portal expõe remessas de outros clientes · OWASP API1 BOLA	Crítica	9,1	Aplicações	Dados pessoais; comunicação à ANPD
C-03	Backups do ERP no mesmo domínio, sem cópia imutável ou offline	Crítica	9,0	Rede interna	Recuperação inviável após ransomware
C-04	Conta de serviço Domain Admin e senha sem troca há 4 anos	Crítica	8,8	Active Directory	Controle total da rede em 3h40
A-05	Bucket S3 público com logs de rastreamento de cargas	Alta	7,5	Nuvem	Exposição de rotas de cargas
A-06	Cobertura de monitoramento insuficiente; logs retidos por 7 dias	Alta	Controle	Detecção	Ataque em curso passaria despercebido
A-07	DMARC p=none; 21% de cliques no phishing simulado	Alta	Controle	E-mail	Fraude e roubo de credenciais
A-08	Rede sem segmentação entre escritórios, CDs e telemetria	Alta	7,2	Rede interna	Ataque alcança a operação física
A-09	Plano de resposta a incidentes nunca testado	Alta	Controle	Processo	Primeiras 24 horas improvisadas
M-10	Fornecedores críticos sem cláusulas de segurança	Média	Controle	Governança	Risco de terceiros fora de controle

100 achados técnicos consolidados em 10 riscos de negócio · dados fictícios

06 · DETALHAMENTO DOS ACHADOS CRÍTICOS

Da entrada pela VPN à interrupção da operação.

Os quatro riscos formam uma cadeia: entrada pela VPN, movimento lateral, escalada de privilégio e destruição dos backups.



Em paralelo, C-02 permite copiar a base de clientes pela internet, sem entrar na rede.

C-01

CRÍTICA

VPN vulnerável e acesso remoto sem MFA

O QUE ENCONTRAMOS	Firmware do concentrador VPN 14 meses desatualizado, com falha de execução remota de código listada no catálogo KEV; 433 de 1.140 usuários acessam sem segundo fator.
EVIDÊNCIA	Versão identificada por fingerprint e confirmada pela equipe de TI. Login bem-sucedido com credencial vazada de um colaborador, sem MFA.
COMO UM ATACANTE USARIA	Credenciais vazadas são vendidas em fóruns. Com elas, o atacante entra na rede como funcionário legítimo.
RECOMENDAÇÃO	Atualizar o firmware em até 72 horas; exigir MFA resistente a phishing para 100% dos acessos e bloquear logins de países fora da operação.
ESFORÇO / DONO	Baixo · Infraestrutura

06 · DETALHAMENTO DOS ACHADOS CRÍTICOS

Dados expostos e recuperação sem proteção.

Dois caminhos de impacto distintos: vazamento pela API e perda da capacidade de restauração após ransomware.

C-02 CRÍTICA

API do portal expõe dados de outros clientes

O QUE ENCONTRAMOS	O endpoint de consulta de remessas aceita qualquer número de pedido, sem verificar se pertence ao cliente autenticado.
EVIDÊNCIA	Com a conta de teste, foram lidos 5 registros de outros clientes. A coleta foi interrompida e os dados, descartados no cenário simulado.
COMO UM ATACANTE USARIA	Um script percorre a sequência de pedidos e copia toda a base em poucas horas.
RECOMENDAÇÃO	Validar a propriedade do objeto em todas as rotas, usar identificadores não previsíveis e revisar logs dos últimos 6 meses.
ESFORÇO / DONO	Médio · Desenvolvimento

C-03 CRÍTICA

Backups sem proteção contra ransomware

O QUE ENCONTRAMOS	O servidor de backup do ERP está no mesmo domínio Active Directory e usa a mesma conta administrativa; não há cópia imutável nem offline.
EVIDÊNCIA	Com a conta obtida em C-04, a equipe teve permissão de exclusão sobre todos os conjuntos de backup. Nenhum dado foi alterado.
COMO UM ATACANTE USARIA	Grupos de ransomware apagam os backups antes de criptografar, para forçar o pagamento do resgate.
RECOMENDAÇÃO	Adotar a regra 3-2-1-1, isolar o backup do domínio e testar trimestralmente a restauração do ERP com tempo medido.
ESFORÇO / DONO	Médio · Infraestrutura

06 E 07 · PRIVILÉGIO E OBRIGAÇÕES

Controle total da rede e lacunas de conformidade.

A conta de serviço simulada permite escalada total; a falha na API também cria um risco regulatório relevante.

C-04 CRÍTICA

Conta de serviço com poder total sobre a rede

O QUE ENCONTRAMOS	A conta usada pelo sistema de impressão é Domain Admin, com senha de 9 caracteres sem troca desde 2022.
EVIDÊNCIA	A senha foi quebrada offline em 41 minutos (Kerberoasting); o controle total do domínio foi obtido em 3h40 a partir de uma estação comum.
COMO UM ATACANTE USARIA	É uma técnica de escalada de privilégio em redes Windows que pode anteceder um ataque de ransomware.
RECOMENDAÇÃO	Remover o privilégio excessivo, migrar para contas gerenciadas (gMSA) com senha rotativa e criar camadas administrativas no AD.
ESFORÇO / DONO	Baixo · Infraestrutura

7. Conformidade

Requisito	Aderência	Principais lacunas
LGPD · art. 48	Não atende	Sem procedimento para avaliar e comunicar incidente à ANPD no prazo
LGPD · art. 41 e registros	Parcial	Encarregado nomeado; inventário de dados desatualizado desde 2024
ISO/IEC 27001:2022 · Anexo A	Não atende	41 de 93 controles; sem SGSI formal nem auditoria interna
Exigências contratuais de clientes	Atende	Questionários respondidos; sem evidência independente
Pré-requisitos típicos de seguro	Parcial	Falta MFA total, EDR em 100% e backup imutável

O tratamento dos riscos críticos também prepara a organização fictícia para uma futura avaliação ISO 27001; isso não representa certificação ou prazo garantido.

08 · ROTEIRO DE REMEDIAÇÃO

Três fases para fechar a porta, enxergar e comprovar.

Os quatro riscos críticos são tratados nos primeiros 30 dias; as fases seguintes constroem capacidade de detecção, resposta e evidência.

0 A 30 DIAS
Fechar a porta
Nota estimada 71

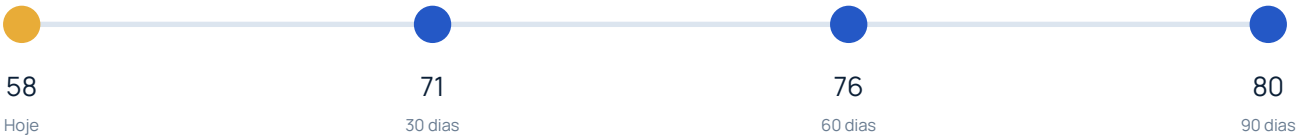
- VPN atualizada + MFA — C-01
- Autorização na API — C-02
- Conta de serviço sem DA — C-04
- Backup imutável do ERP — C-03
- Bucket S3 fechado — A-05

31 A 60 DIAS
Enxergar e reagir
Nota estimada 76

- Monitoramento contínuo — A-06
- Logs por 12 meses — A-06
- DMARC p=reject — A-07
- Treino antiphishing — A-07
- Resposta a incidentes — A-09

61 A 90 DIAS
Estruturar e comprovar
Nota estimada 80

- Rede de CDs segmentada — A-08
- Camadas no AD + EDR — C-04
- Contratos com terceiros — M-10
- Reteste independente
- Relatório à diretoria



Cada ação concluída deve ser validada antes de marcada como resolvida. O reteste do dia 90 gera um novo índice para comparação.

09 · PLATAFORMA E SERVIÇOS CONECTADOS

Cada risco encontra uma frente de atuação.

A organização pode executar internamente o que tiver capacidade e contratar apenas o apoio necessário.

Solução	Entrega prevista no cenário	Achados
CYVORA SENTINEL	Monitoramento com triagem de alertas, caça a ameaças e apoio à resposta	A-06 · A-09
CYVORA OFFENSIVE	Reteste dos críticos, teste das APIs e reteste completo no dia 90	C-01 · C-02 · C-04
CYVORA CLOUD	Revisão de AWS e M365, backup imutável e segmentação da rede	C-03 · A-05 · A-08
CYVORA GOVERNANCE	Programa LGPD, comunicação à ANPD, fornecedores e preparação ISO	M-10 · seção 7
CYVORA INTELLIGENCE	Monitoramento de credenciais vazadas e menções à marca	C-01 · A-07
CYVORA ONE	Visão executiva da postura, evolução do plano e indicadores	Todos

PRÓXIMO PASSO NO CENÁRIO

Reunião de 60 minutos com TI, jurídico e operações para validar responsáveis e iniciar a fase de 30 dias.

A cobertura e os horários de monitoramento são definidos conforme a operação contratada e validada para cada projeto.

ANEXO

Critérios comuns para uma conversa objetiva.

Severidade técnica, contexto de negócio e prazos recomendados apresentados de forma transparente.

Severidade	CVSS 3.1	Critério CYVORA	Prazo recomendado
Crítica	9,0 a 10,0	Explorável remotamente ou listada no KEV, com impacto direto na operação ou em dados pessoais	Até 7 dias
Alta	7,0 a 8,9	Explorável com algum pré-requisito, ou falha de controle que amplia um ataque	Até 30 dias
Média	4,0 a 6,9	Requer condições específicas ou tem impacto limitado	Até 90 dias
Baixa	0,1 a 3,9	Boa prática ou risco residual	Próximo ciclo

GLOSSÁRIO

BOLA — Falha de autorização em que um usuário acessa objetos de outro usuário.

CVSS — Escala internacional de 0 a 10 para a gravidade técnica de uma vulnerabilidade.

DMARC — Política de e-mail que ajuda a impedir o uso indevido do domínio em mensagens falsas.

gMSA — Conta de serviço do Windows com senha longa trocada automaticamente.

Kerberoasting — Técnica que extrai e quebra offline a senha de contas de serviço do AD.

KEV — Catálogo da CISA com vulnerabilidades já exploradas em ataques reais.

MFA — Autenticação com mais de um fator, como senha e aplicativo ou chave física.

SOC — Centro de operações de segurança que monitora e responde a alertas.

AVISO DE DEMONSTRAÇÃO

Empresa, números, evidências e achados são fictícios. O documento é uma amostra pública de estrutura e profundidade, não um diagnóstico real ou garantia de resultado.