MAIO 2026

Penetration Testing Report Details PTBR

Teste de Intrusão em Ambiente FÁCIL

Cliente	FÁCIL
Tipo de teste	Blackbox / superfície externa, firewall, cloud e serviços publicados
Documento	Relatório técnico de Penetration Testing
Preparado por	Microtech
Data	Maio de 2026

Conteúdo

1. Aviso Legal

1.1 Isenção de Responsabilidade

Reconhece-se a impossibilidade de testar redes, sistemas, serviços e aplicações contra todas as potenciais vulnerabilidades de segurança. Este relatório, portanto, não pode garantir proteção integral dos ativos contra todas as ameaças existentes.

Os testes realizados refletem a perspectiva técnica da Microtech no período de avaliação e os problemas identificados são específicos ao contexto, escopo e evidências disponíveis. Considerando a natureza dinâmica da tecnologia da informação, vulnerabilidades desconhecidas ou surgidas após o período de avaliação podem não estar contempladas neste documento.

As recomendações descritas têm como finalidade apoiar o processo de mitigação, priorização e melhoria da postura de segurança. A implementação deve considerar janela de mudança, impacto operacional, dependências de terceiros e validação em ambiente controlado quando aplicável.

1.2 Declaração de Confidencialidade

Este documento contém informações proprietárias e confidenciais da FÁCIL e da Microtech. A divulgação, reprodução, distribuição ou compartilhamento total ou parcial deve ocorrer somente mediante autorização das partes envolvidas e para fins de tratativa técnica, auditoria, conformidade ou gestão de riscos.

O conteúdo pode conter endereços de rede, serviços, vulnerabilidades, riscos e recomendações que, se divulgados indevidamente, podem ampliar a exposição do ambiente. Recomenda-se armazenamento seguro e distribuição restrita aos responsáveis pela tomada de decisão e correção técnica.

2. Introdução

A Microtech conduziu um teste de intrusão no ambiente da FÁCIL com o objetivo de avaliar a postura de segurança dos ativos definidos em escopo, identificar vulnerabilidades técnicas e apresentar recomendações de mitigação priorizadas por risco.

O teste contemplou a análise de superfície externa, firewall local, firewall cloud, regras de NAT/publicação, IPs públicos, servidores cloud, VPN e serviços publicados, com foco em identificar condições que possam impactar confidencialidade, integridade, disponibilidade, continuidade operacional ou reputação da organização.

O processo seguiu etapas de reconhecimento, enumeração de ativos e serviços, identificação de vulnerabilidades, validação técnica e documentação dos resultados. Quando aplicável, foram adotadas precauções para reduzir risco de indisponibilidade ou impacto operacional.

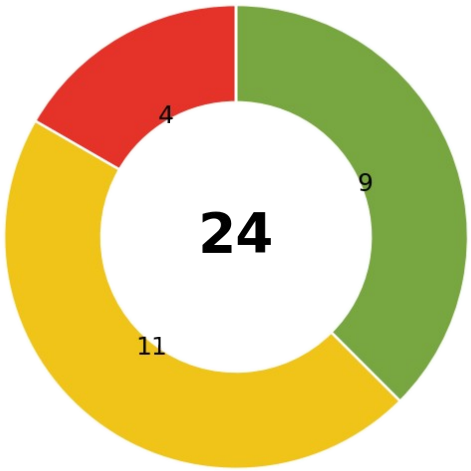
Este relatório deve ser utilizado como base para planejamento de correções, priorização de ações técnicas, reteste e evolução contínua dos controles de segurança do ambiente.

3. Sumário Executivo

A avaliação identificou vulnerabilidades relacionadas principalmente a serviços publicados, FreePBX, sistema operacional em fim de vida, componentes desatualizados, publicações NAT, configuração de VPN e endurecimento de serviços cloud.

Foram consolidadas 24 vulnerabilidades, classificadas da seguinte forma: 0 críticas, 4 altas, 11 médias, 9 baixas e 0 informativas. As vulnerabilidades de maior prioridade estão associadas ao IP público 186.237.145.229, ao serviço FreePBX e ao uso de sistema operacional CentOS 7 em fim de vida.

A recomendação principal é iniciar a mitigação pelos itens de severidade Alta, principalmente redução de exposição do FreePBX, atualização/substituição de componentes sem suporte, revisão de NATs/publicações e fortalecimento de acesso remoto com MFA, restrição de origem e monitoramento.



Total de vulnerabilidades: 24

Crítica: 0	Alta: 4	Média: 11	Baixa: 9	Informativa: 0

4. Escopo

O modelo de teste adotado foi Blackbox, simulando a perspectiva de um atacante externo com informações limitadas sobre o ambiente. A análise se concentrou em identificar ativos acessíveis, serviços expostos, configurações potencialmente frágeis e vulnerabilidades conhecidas.

Ambiente	Produção
Tipo	Blackbox / segurança ofensiva controlada
Acesso ao código fonte	Não
Escopo principal	Firewall local, firewall cloud, IPs públicos, servidores cloud, VPN, NATs/publicações e FreePBX
Ativos observados	186.237.145.229; 10.150.100.1; servidores cloud 172.16.10.x; VPN SSL; publicações NAT

Fora do Escopo

Não foram considerados no escopo ataques de engenharia social, phishing contra usuários, negação de serviço distribuída (DDoS), exploração destrutiva, alteração de dados produtivos ou testes que pudessem causar indisponibilidade sem aprovação prévia.

4.1 Metodologia

Reconhecimento e enumeração

Identificação de hosts, portas, protocolos, banners, tecnologias, serviços publicados e caminhos de exposição externa.

Identificação de vulnerabilidades

Correlação de serviços e versões com vulnerabilidades conhecidas, revisão de configurações, exposição de portas, hardening e presença de componentes em fim de vida.

Validação técnica

Validação da existência das vulnerabilidades reportadas, evitando falsas classificações sempre que possível e respeitando limites de segurança operacional.

Análise de impacto

Avaliação do potencial impacto para confidencialidade, integridade, disponibilidade, continuidade operacional e exposição de dados.

Priorização

Classificação por severidade, exposição, criticidade do ativo, facilidade de exploração, impacto de negócio e necessidade de correção.

Relato e recomendação

Documentação dos achados com ativos afetados, recomendações técnicas, referências e critérios de reteste.

A metodologia foi alinhada a práticas reconhecidas como PTES (Penetration Testing Execution Standard), NIST SP 800-115 e uso complementar de referência CVSS para categorização de severidade.

5. Classificações de Riscos

A categorização de risco utilizada neste relatório considera a severidade técnica, a exposição do ativo, o contexto de negócio e a possibilidade de exploração. O CVSS é utilizado como referência geral, complementado por avaliação contextual do ambiente FÁCIL.

Severidade	CVSS	Descrição
Crítica	9.0 - 10.0	Pode permitir comprometimento direto, amplo ou imediato de sistemas, dados ou operação. Deve ser tratada imediatamente.
Alta	7.0 - 8.9	Pode permitir comprometimento relevante do ativo ou serviço, especialmente quando exposto externamente.
Média	4.0 - 6.9	Exige atenção e correção planejada. Pode ampliar risco quando combinada a outras falhas ou exposição.
Baixa	0.1 - 3.9	Não representa risco imediato isolado, mas contribui para enumeração, exposição ou fragilidade acumulada.
Informativa	0.0	Não representa vulnerabilidade direta, mas indica informação útil para melhoria da postura de segurança.

6. Tabela de Vulnerabilidades

A tabela a seguir apresenta o resumo das vulnerabilidades identificadas durante o teste, acompanhadas de severidade, status e ativo/camada afetada.

6.1 Vulnerabilidades - Parte 1

ID	Vulnerabilidade	Severidade	Status	Ativo afetado
PT_FACIL_001	FreePBX vulnerável a execução remota de comandos	Alta	Não corrigido	186.237.145.229:8192/tcp
PT_FACIL_002	FreePBX com bypass de autenticação administrativa	Alta	Não corrigido	186.237.145.229
PT_FACIL_003	FreePBX vulnerável a execução remota de código	Alta	Não corrigido	186.237.145.229
PT_FACIL_004	Sistema operacional CentOS 7 em fim de vida	Alta	Não corrigido	186.237.145.229
PT_FACIL_005	Gerenciamento de patches insuficiente - OpenSSH	Média	Não corrigido	186.237.145.229:22/tcp
PT_FACIL_006	Gerenciamento de patches insuficiente - Apache	Média	Não corrigido	186.237.145.229:80/tcp
PT_FACIL_007	Gerenciamento de patches insuficiente - MySQL/MariaDB	Média	Não corrigido	186.237.145.229:3306/tcp
PT_FACIL_008	Gerenciamento de patches insuficiente - PHP	Média	Não corrigido	186.237.145.229
PT_FACIL_009	Ausência de proteção por geolocalização na VPN	Média	Não corrigido	Firewall Local / VPN SSL
PT_FACIL_010	Ausência de segundo fator de autenticação na VPN	Média	Não corrigido	Firewall Local / VPN SSL
PT_FACIL_011	VPN permite múltiplas conexões simultâneas por usuário	Média	Não corrigido	Firewall Local / VPN SSL
PT_FACIL_012	Publicações NAT demandam revisão e justificativa	Média	Não corrigido	Firewall Local / NAT

6.2 Vulnerabilidades - Parte 2

ID	Vulnerabilidade	Severidade	Status	Ativo afetado
PT_FACIL_013	Uso de TLS e parâmetros de serviço passíveis de endurecimento	Média	Não corrigido	Firewall Cloud 10.150.100.1
PT_FACIL_014	Serviço RDP requer hardening e restrição de acesso	Média	Não corrigido	Servidores Cloud / 3389/tcp
PT_FACIL_015	Serviços RPC/Windows requerem restrição de origem	Média	Não corrigido	Servidores Cloud / 135/tcp
PT_FACIL_016	Serviços acessíveis externamente com necessidade de revisão	Baixa	Não corrigido	Ambiente Externo
PT_FACIL_017	Padronização e endurecimento de servidores cloud	Baixa	Não corrigido	Servidores Cloud 172.16.10.x
PT_FACIL_018	Revisão de origens permitidas em regras publicadas	Baixa	Não corrigido	Firewall Local / NAT
PT_FACIL_019	Inventário de serviços expostos insuficiente	Baixa	Não corrigido	Ambiente Externo
PT_FACIL_020	Resposta ICMP habilitada em ativos expostos	Baixa	Não corrigido	IPs públicos / Cloud
PT_FACIL_021	Banners e informações de serviço expostas	Baixa	Não corrigido	Serviços publicados
PT_FACIL_022	Cadeia de certificados e parâmetros TLS requerem revisão periódica	Baixa	Não corrigido	Serviços TLS
PT_FACIL_023	Portas abertas sem documentação operacional completa	Baixa	Não corrigido	Firewall Local / Cloud
PT_FACIL_024	Logs e evidências de segurança sem centralização formal	Baixa	Não corrigido	Ambiente de Segurança

7. Detalhes das Vulnerabilidades

Nas páginas a seguir encontram-se os detalhes de cada vulnerabilidade identificada durante o processo de Penetration Testing.

PT_FACIL_001 - FreePBX vulnerável a execução remota de comandos

Severidade	CVSS estimado	CWE	Status
Alta	**8.1**	**CWE-78**	**Não corrigido**

Descrição e impacto

Serviço FreePBX publicado externamente com potencial de exploração remota.

Esta vulnerabilidade deve ser priorizada por estar associada a serviço exposto, componente sem suporte ou possibilidade de comprometimento relevante do ativo afetado.

Ativos afetados

186.237.145.229:8192/tcp

Recomendações

- Atualizar FreePBX e módulos.
- restringir origem no firewall.
- validar necessidade da publicação.
- revisar logs e credenciais.
- executar reteste após correção.

Referências

https://cwe.mitre.org/data/definitions/78.html

PT_FACIL_002 - FreePBX com bypass de autenticação administrativa

Severidade	CVSS estimado	CWE	Status
Alta	**8.1**	**CWE-287**	**Não corrigido**

Descrição e impacto

Possibilidade de contorno de autenticação administrativa em serviço exposto.

Esta vulnerabilidade deve ser priorizada por estar associada a serviço exposto, componente sem suporte ou possibilidade de comprometimento relevante do ativo afetado.

Ativos afetados

186.237.145.229

Recomendações

- Bloquear administração direta pela internet.
- atualizar o FreePBX.
- restringir acesso via VPN/IPs confiáveis.
- revisar contas administrativas e senhas.

Referências

https://cwe.mitre.org/data/definitions/287.html

PT_FACIL_003 - FreePBX vulnerável a execução remota de código

Severidade	CVSS estimado	CWE	Status
Alta	**8.1**	**CWE-94**	**Não corrigido**

Descrição e impacto

Falha com potencial de execução de código em serviço publicado.

Esta vulnerabilidade deve ser priorizada por estar associada a serviço exposto, componente sem suporte ou possibilidade de comprometimento relevante do ativo afetado.

Ativos afetados

186.237.145.229

Recomendações

- Atualizar aplicação e dependências.
- isolar serviço.
- aplicar allowlist de origem.
- revisar módulos e realizar varredura pós-correção.

Referências

https://cwe.mitre.org/data/definitions/94.html

PT_FACIL_004 - Sistema operacional CentOS 7 em fim de vida

Severidade	CVSS estimado	CWE	Status
Alta	**8.1**	**CWE-1104**	**Não corrigido**

Descrição e impacto

Sistema operacional sem ciclo regular de correções oficiais, elevando a exposição a vulnerabilidades conhecidas.

Esta vulnerabilidade deve ser priorizada por estar associada a serviço exposto, componente sem suporte ou possibilidade de comprometimento relevante do ativo afetado.

Ativos afetados

186.237.145.229

Recomendações

- Planejar migração para distribuição suportada.
- validar compatibilidade.
- criar backup.
- testar em homologação.
- desativar sistema legado após migração.

Referências

https://cwe.mitre.org/data/definitions/1104.html

PT_FACIL_005 - Gerenciamento de patches insuficiente - OpenSSH

Severidade	CVSS estimado	CWE	Status
Média	**5.3**	**CWE-1104**	**Não corrigido**

Descrição e impacto

Versão/componente de acesso remoto requer revisão de atualização e hardening.

Ativos afetados

186.237.145.229:22/tcp

Recomendações

- Atualizar OpenSSH.
- restringir origem por firewall.
- desabilitar login root.
- priorizar chaves SSH.
- registrar exceções.

Referências

https://nvd.nist.gov/

PT_FACIL_006 - Gerenciamento de patches insuficiente - Apache

Severidade	CVSS estimado	CWE	Status
Média	**5.3**	**CWE-1104**	**Não corrigido**

Descrição e impacto

Componente web identificado com necessidade de atualização e revisão de exposição.

Ativos afetados

186.237.145.229:80/tcp

Recomendações

- Atualizar Apache.
- remover módulos não utilizados.
- ocultar banners.
- revisar virtual hosts e diretórios expostos.

Referências

https://httpd.apache.org/security/

PT_FACIL_007 - Gerenciamento de patches insuficiente - MySQL/MariaDB

Severidade	CVSS estimado	CWE	Status
Média	**5.3**	**CWE-1104**	**Não corrigido**

Descrição e impacto

Banco de dados associado a componente legado requer atualização e revisão de exposição.

Ativos afetados

186.237.145.229:3306/tcp

Recomendações

- Atualizar banco.
- garantir que não esteja exposto externamente.
- revisar usuários, permissões e senhas.
- realizar backup antes da alteração.

Referências

https://www.cvedetails.com/

PT_FACIL_008 - Gerenciamento de patches insuficiente - PHP

Severidade	CVSS estimado	CWE	Status
Média	**5.3**	**CWE-1104**	**Não corrigido**

Descrição e impacto

Versão/dependências PHP requerem atualização conforme compatibilidade da aplicação.

Ativos afetados

186.237.145.229

Recomendações

- Atualizar PHP.
- validar compatibilidade com FreePBX.
- remover extensões não utilizadas.
- revisar parâmetros de segurança.

Referências

https://www.php.net/supported-versions.php

PT_FACIL_009 - Ausência de proteção por geolocalização na VPN

Severidade	CVSS estimado	CWE	Status
Média	**5.3**	**CWE-693**	**Não corrigido**

Descrição e impacto

Acesso remoto exposto sem restrição geográfica pode ampliar tentativas indevidas de autenticação.

Ativos afetados

Firewall Local / VPN SSL

Recomendações

- Aplicar bloqueio por país quando viável.
- liberar apenas regiões necessárias.
- monitorar tentativas negadas.
- combinar com MFA.

Referências

https://attack.mitre.org/

PT_FACIL_010 - Ausência de segundo fator de autenticação na VPN

Severidade	CVSS estimado	CWE	Status
Média	**5.3**	**CWE-308**	**Não corrigido**

Descrição e impacto

VPN sem MFA aumenta risco em caso de credenciais comprometidas.

Ativos afetados

Firewall Local / VPN SSL

Recomendações

- Habilitar MFA para VPN.
- priorizar usuários administrativos.
- revisar grupos de acesso.
- registrar exceções temporárias.

Referências

https://cwe.mitre.org/data/definitions/308.html

PT_FACIL_011 - VPN permite múltiplas conexões simultâneas por usuário

Severidade	CVSS estimado	CWE	Status
Média	**5.3**	**CWE-287**	**Não corrigido**

Descrição e impacto

Sessões concorrentes podem dificultar rastreabilidade e aumentar abuso de credenciais.

Ativos afetados

Firewall Local / VPN SSL

Recomendações

- Definir limite de sessão por usuário.
- monitorar acessos concorrentes.
- revisar política por grupo.
- gerar alertas de comportamento anômalo.

Referências

https://owasp.org/www-project-top-10-infrastructure-security-risks/

PT_FACIL_012 - Publicações NAT demandam revisão e justificativa

Severidade	CVSS estimado	CWE	Status
Média	**5.3**	**CWE-284**	**Não corrigido**

Descrição e impacto

Regras de publicação podem ampliar superfície externa se não houver controle de origem e justificativa documentada.

Ativos afetados

Firewall Local / NAT

Recomendações

- Inventariar NATs.
- confirmar necessidade operacional.
- remover publicações não utilizadas.
- restringir origem por IP.
- documentar responsável.

Referências

https://owasp.org/www-project-top-10-infrastructure-security-risks/

PT_FACIL_013 - Uso de TLS e parâmetros de serviço passíveis de endurecimento

Severidade	CVSS estimado	CWE	Status
Média	**5.3**	**CWE-326**	**Não corrigido**

Descrição e impacto

Parâmetros criptográficos e exposição de serviços devem ser revisados para fortalecer confidencialidade e integridade.

Ativos afetados

Firewall Cloud 10.150.100.1

Recomendações

- Desabilitar protocolos antigos.
- remover cifras fracas.
- validar certificado/cadeia.
- aplicar hardening TLS e retestar.

Referências

https://cwe.mitre.org/data/definitions/326.html

PT_FACIL_014 - Serviço RDP requer hardening e restrição de acesso

Severidade	CVSS estimado	CWE	Status
Média	**5.3**	**CWE-284**	**Não corrigido**

Descrição e impacto

Serviço de acesso remoto deve operar com NLA, restrição de origem e auditoria ativa.

Ativos afetados

Servidores Cloud / 3389/tcp

Recomendações

- Habilitar NLA.
- restringir por VPN/IPs confiáveis.
- auditar tentativas.
- revisar necessidade de exposição.

Referências

https://attack.mitre.org/techniques/T1021/001/

PT_FACIL_015 - Serviços RPC/Windows requerem restrição de origem

Severidade	CVSS estimado	CWE	Status
Média	**5.3**	**CWE-284**	**Não corrigido**

Descrição e impacto

Serviços administrativos de Windows podem aumentar superfície interna/cloud se não houver filtros adequados.

Ativos afetados

Servidores Cloud / 135/tcp

Recomendações

- Restringir portas administrativas.
- aplicar firewall local.
- permitir apenas redes de gestão.
- monitorar acessos.

Referências

https://learn.microsoft.com/windows/security/

PT_FACIL_016 - Serviços acessíveis externamente com necessidade de revisão

Severidade	CVSS estimado	CWE	Status
Baixa	**2.6**	**CWE-200**	**Não corrigido**

Descrição e impacto

Serviços expostos devem ser revisados quanto à necessidade, proprietário e controle de origem.

Ativos afetados

Ambiente Externo

Recomendações

- Inventariar serviços.
- desativar itens sem uso.
- registrar responsável.
- aplicar allowlist quando possível.

Referências

https://owasp.org/www-project-top-10-infrastructure-security-risks/

PT_FACIL_017 - Padronização e endurecimento de servidores cloud

Severidade	CVSS estimado	CWE	Status
Baixa	**2.6**	**CWE-693**	**Não corrigido**

Descrição e impacto

Ausência de baseline formal pode resultar em variações de configuração e lacunas de hardening.

Ativos afetados

Servidores Cloud 172.16.10.x

Recomendações

- Criar baseline de hardening.
- padronizar firewall local, logs, atualizações, antivírus/EDR e serviços habilitados.

Referências

https://www.cisecurity.org/cis-benchmarks

PT_FACIL_018 - Revisão de origens permitidas em regras publicadas

Severidade	CVSS estimado	CWE	Status
Baixa	**2.6**	**CWE-284**	**Não corrigido**

Descrição e impacto

Regras sem allowlist podem expor serviços a origens não relacionadas ao negócio.

Ativos afetados

Firewall Local / NAT

Recomendações

- Identificar IPs autorizados.
- remover origem any quando não necessária.
- revisar allowlists periodicamente.

Referências

https://owasp.org/www-project-top-10-infrastructure-security-risks/

PT_FACIL_019 - Inventário de serviços expostos insuficiente

Severidade	CVSS estimado	CWE	Status
Baixa	**2.6**	**CWE-1059**	**Não corrigido**

Descrição e impacto

A ausência de inventário completo prejudica governança, resposta a incidentes e gestão de mudanças.

Ativos afetados

Ambiente Externo

Recomendações

- Registrar IP, porta, destino interno, dono, justificativa, origem permitida e data de revisão.

Referências

https://www.iso.org/standard/27001

PT_FACIL_020 - Resposta ICMP habilitada em ativos expostos

Severidade	CVSS estimado	CWE	Status
Baixa	**2.6**	**CWE-200**	**Não corrigido**

Descrição e impacto

Resposta a ICMP pode auxiliar enumeração de ativos, embora não represente comprometimento direto.

Ativos afetados

IPs públicos / Cloud

Recomendações

- Avaliar necessidade.
- limitar ICMP por origem quando possível.
- manter monitoramento sem ampliar exposição pública.

Referências

https://owasp.org/

PT_FACIL_021 - Banners e informações de serviço expostas

Severidade	CVSS estimado	CWE	Status
Baixa	**2.6**	**CWE-200**	**Não corrigido**

Descrição e impacto

Banners podem revelar tecnologia e versões, facilitando enumeração por atacantes.

Ativos afetados

Serviços publicados

Recomendações

- Reduzir banners.
- ocultar versão.
- padronizar mensagens.
- validar cabeçalhos e respostas de serviços.

Referências

https://cwe.mitre.org/data/definitions/200.html

PT_FACIL_022 - Cadeia de certificados e parâmetros TLS requerem revisão periódica

Severidade	CVSS estimado	CWE	Status
Baixa	**2.6**	**CWE-295**	**Não corrigido**

Descrição e impacto

Certificados, cadeias e expiração devem ser acompanhados para reduzir indisponibilidade e falhas de confiança.

Ativos afetados

Serviços TLS

Recomendações

- Implementar alerta de expiração.
- validar chain.
- renovar certificados antes do vencimento.
- usar protocolos atuais.

Referências

https://cwe.mitre.org/data/definitions/295.html

PT_FACIL_023 - Portas abertas sem documentação operacional completa

Severidade	CVSS estimado	CWE	Status
Baixa	**2.6**	**CWE-284**	**Não corrigido**

Descrição e impacto

Portas abertas sem documentação dificultam análise de risco e aprovação de mudanças.

Ativos afetados

Firewall Local / Cloud

Recomendações

- Criar matriz de publicação.
- revisar mensalmente.
- remover portas sem dono.
- validar com áreas de negócio.

Referências

https://owasp.org/

PT_FACIL_024 - Logs e evidências de segurança sem centralização formal

Severidade	CVSS estimado	CWE	Status
Baixa	**2.6**	**CWE-778**	**Não corrigido**

Descrição e impacto

A ausência de centralização reduz capacidade de correlação e investigação pós-incidente.

Ativos afetados

Ambiente de Segurança

Recomendações

- Centralizar logs de firewall, VPN, servidores e serviços.
- criar retenção mínima.
- configurar alertas por severidade.

Referências

https://cwe.mitre.org/data/definitions/778.html

8. Plano de Correção e Priorização

Prazo	Objetivo	Ações
Imediato	Reduzir risco alto	FreePBX exposto, vulnerabilidades RCE/auth bypass e CentOS 7 EOL. Aplicar restrição de origem e plano de atualização/migração.
Curto prazo	Fortalecer acesso remoto	Implantar MFA na VPN, revisar múltiplas sessões, geolocalização e políticas de acesso.
Curto prazo	Revisar publicações	Inventariar NATs, portas publicadas e origens permitidas no firewall local e cloud.
Médio prazo	Patch management	Criar ciclo de patches, inventário de versões, homologação e janela de atualização.
Médio prazo	Hardening cloud	Aplicar baseline de segurança em servidores cloud, TLS, firewall local, serviços e logs.
Após correções	Reteste	Executar nova avaliação para confirmar mitigação e atualizar status das vulnerabilidades.

9. Critérios de Aceite e Reteste

- Evidência de atualização ou mitigação aplicada para cada vulnerabilidade.
- Revisão de regras de firewall/NAT com responsável, origem permitida e justificativa.
- Validação de que serviços administrativos não estão expostos sem restrição.
- Comprovação de MFA habilitado para VPN ou registro formal de exceção.
- Execução de reteste técnico para alteração de status para Corrigido ou Risco Aceito formalmente.