Gestão de Riscos Executiva

Diagnóstico Técnico e Pentest - Ambiente FÁCIL

Documento final executivo consolidado com diagnóstico geral, classificação do ambiente, principais problemas identificados, vulnerabilidades do Pentest e recomendações Microtech.

Síntese executiva

O cliente aprovou duas frentes de atuação: análise técnica do ambiente, com mapeamento geral da infraestrutura e validação dos problemas relatados, e execução de Pentest, com identificação de vulnerabilidades na superfície avaliada. O resultado aponta um ambiente operacional e estruturado, porém com necessidade de evolução contínua em governança, monitoramento, gestão de patches, exposição de serviços e gestão preventiva de riscos.

Item	Resumo executivo
Propostas aprovadas	1) Análise técnica do ambiente geral. 2) Execução de Pentest.
Classificação geral	Médio, com pontos pontuais de criticidade alta.
Prioridade de ação	Alta, com plano de correção e acompanhamento mensal.
Foco principal	Reduzir exposição, corrigir vulnerabilidades, estabilizar acesso remoto, fortalecer monitoramento e governança.

1. Contexto e escopo aprovado

A avaliação foi conduzida a partir de duas frentes aprovadas pela FÁCIL: uma análise técnica do ambiente geral e a execução de Pentest. As frentes são complementares: a análise técnica avalia operação, infraestrutura, sintomas relatados e riscos de sustentação; o Pentest avalia vulnerabilidades e exposição de segurança.

Frente aprovada	Objetivo	Resultado esperado
Análise técnica	Mapear a infraestrutura geral, validar problemas relatados, avaliar operação, TSplus/RDP, VPN, servidores, cloud, firewall, NATs e serviços críticos.	Identificação de problemas, riscos operacionais, gargalos e recomendações de melhoria.
Pentest	Validar a superfície exposta e identificar vulnerabilidades em IPs, serviços publicados, firewall, NATs, FreePBX e componentes acessíveis.	Classificação de vulnerabilidades, priorização de correções e redução de exposição.

Leitura executiva

A avaliação não deve ser interpretada como um ponto isolado, mas como base para criação de um ciclo contínuo de gestão de riscos, com acompanhamento mensal, responsáveis, prazos, validação de correções e indicadores visíveis para a Diretoria.

2. Diagnóstico executivo geral

O ambiente possui infraestrutura presente e capacidade operacional, incluindo firewall, VPN, servidores, cloud, links e serviços publicados. Porém, foram identificados riscos técnicos e operacionais que precisam ser acompanhados de forma contínua, principalmente em segurança, acesso remoto, monitoramento, atualização de componentes e governança.

Eixo	Condição observada	Risco executivo
Infraestrutura	Ambiente com base técnica funcional, servidores, firewall, VPN, cloud e serviços de sustentação.	A infraestrutura sustenta a operação, mas requer padronização e revisão recorrente.
Segurança	Vulnerabilidades altas em serviço exposto, componentes desatualizados e necessidade de revisão de publicações/NAT.	Possibilidade de exploração externa, indisponibilidade ou comprometimento de serviço.
Acesso remoto	TSplus/RDP, VPN, áudio, microfone, USB e VoIP dependem de múltiplas camadas sensíveis.	Instabilidade pode ser percebida pelo usuário como falha da aplicação, mesmo quando a origem está em rede, redirecionamento ou recursos locais.
Governança	Necessidade de rotina formal de gestão de riscos, patches, revisão mensal e comitê de crise/melhoria.	Riscos podem se acumular sem visibilidade executiva.
Monitoramento	Necessidade de dashboard em tempo real, triggers e alertas para sistemas críticos.	Problemas podem ser percebidos apenas após impacto ao usuário.

3. Classificação geral do ambiente

Critério	Classificação / leitura executiva
Classificação geral	Médio
Nível de risco	Médio, com vulnerabilidades e riscos pontuais de alta criticidade.
Condição operacional	Ambiente funcional, estruturado e com infraestrutura presente.

Critério	Classificação / leitura executiva
Ponto central de evolução	Governança contínua, monitoramento ativo, gestão de patches, controle de exposição e resposta a incidentes.
Prioridade	Alta para correções críticas e criação de rotina mensal de revisão.

A classificação considera que a infraestrutura possui recursos técnicos e sustentação operacional. Ao mesmo tempo, a presença de vulnerabilidades altas, riscos de acesso remoto, componentes em fim de vida e ausência de um processo recorrente de revisão indicam necessidade de amadurecimento na gestão contínua do ambiente.

4. Problemas identificados na análise técnica

A análise técnica mapeou problemas relatados e evidências observadas no ambiente. Os pontos abaixo representam riscos operacionais e de continuidade que precisam ser tratados em conjunto com as correções de segurança.

Tema	Problema identificado	Impacto potencial	Recomendação
TSplus/RDP	Indícios de sensibilidade nos canais virtuais de RDP/TSplus, principalmente com áudio, microfone, USB e VoIP redirecionados.	Falhas perceptíveis de áudio, microfone, reconexões, travamentos pontuais e instabilidade para usuários em home office.	Reduzir redirecionamentos, testar estabilidade por etapas e avaliar alternativas para telefonia fora da sessão TSplus.
Home office	A experiência depende de múltiplas camadas: internet do usuário, Wi-Fi local, máquina, headset/USB, VPN, RDP/TSplus e servidor.	A causa do problema pode não estar apenas no servidor; qualquer camada pode afetar áudio, sessão e CRM.	Criar requisitos mínimos para rede home office e checklist de validação do usuário.
CRM Gestão / Discador	Quando o Discador/VoIP falha dentro do TSplus, o CRM Gestão é impactado operacionalmente.	Usuários podem ficar sem realizar ou receber chamadas, com impacto em cobrança, atendimento, produtividade e continuidade da operação.	Reavaliar arquitetura do Discador/VoIP, separar telefonia da sessão remota quando viável e homologar alternativa estável.
Memória TSplus	Uso de memória observado em patamares elevados, chegando próximo ao limite.	Menor folga para cache, paginação e aumento de usuários simultâneos.	Avaliar aumento do servidor TSplus para 45 GB e monitorar comportamento após ajuste.
Disco / desempenho	Indícios de picos de gravação e consumo de disco em momentos específicos.	Lentidão, perda de responsividade e agravamento de instabilidades em sessões remotas.	Monitorar disco SAS, processos causadores e avaliar melhoria de armazenamento se persistir.
Firewall / NAT	Publicações e regras de NAT demandam revisão de necessidade, origem e exposição.	Aumento de superfície de ataque e risco de publicação indevida.	Revisar regras, documentar finalidade, restringir origem e remover publicações sem uso.

4.1 Sensibilidade das camadas no home office

Camada	Exemplo de falha	Efeito percebido pelo usuário
Internet do usuário	Oscilação, perda de pacotes, latência ou upload limitado.	Reconexões, áudio picotando e lentidão.
Wi-Fi / rede local	Sinal fraco, roteador instável ou múltiplos dispositivos concorrendo.	Quedas curtas que afetam RDP e VoIP.
Equipamento do usuário	Drivers, headset USB, energia, performance local.	Microfone ou áudio falhando dentro da sessão.
VPN	Perda momentânea de túnel ou rota.	Interrupção da sessão remota e sistemas publicados.
TSplus/RDP	Fechamento/reabertura de canais virtuais, redirecionamento de áudio/USB.	Falha de áudio, microfone, VoIP e reconexões.
Servidor / CRM / Discador	Carga, memória, disco, aplicação ou serviço de telefonia.	Impacto direto no CRM Gestão e operação de atendimento/cobrança.

5. Vulnerabilidades identificadas no Pentest

O Pentest identificou vulnerabilidades que exigem priorização, especialmente em serviços expostos e componentes sem suporte. As vulnerabilidades de alta severidade devem ser tratadas com prioridade, seguidas pela revisão das exposições e endurecimento das camadas de acesso.

Host / Camada	Severidade	Vulnerabilidades / Pontos identificados	Ação recomendada
IP público 186.237.145.229	Alta	FreePBX vulnerável a execução remota de comandos/código e bypass de autenticação administrativa.	Corrigir/atualizar FreePBX, restringir origem, revisar exposição e validar necessidade da publicação.
IP público 186.237.145.229	Alta	Sistema operacional CentOS 7 em fim de vida.	Planejar migração para sistema operacional suportado e validar compatibilidade da aplicação.
IP público 186.237.145.229	Média	Gerenciamento de patches insuficiente em OpenSSH, Apache, MySQL e PHP.	Atualizar componentes, aplicar hardening e revisar dependências.
Firewall local / VPN SSL	Média	Ausência de MFA, geolocalização e controle de múltiplas conexões simultâneas.	Implementar MFA, revisar política de acesso e restringir origem quando aplicável.
Firewall local / NAT	Média	Publicações e NATs requerem revisão de exposição.	Mapear regras, remover exceções sem uso, restringir origem e documentar finalidade.
Firewall cloud / Serviços	Média	Parâmetros TLS e serviços passíveis de endurecimento.	Aplicar hardening, remover protocolos antigos e validar configurações.

6. Recomendação Microtech

A recomendação da Microtech é transformar os pontos levantados em um ciclo recorrente de gestão, evitando que as correções sejam tratadas apenas como ações pontuais. O foco deve ser continuidade operacional, segurança preventiva, visibilidade executiva e melhoria contínua.

Pilar	Recomendação	Resultado esperado
Gestão de patches	Padronizar automação de patches com regras, janelas, periodicidade, exceções documentadas e validação pós-atualização.	Redução de vulnerabilidades por componentes desatualizados.
Monitoramento ativo	Implantar dashboard em tempo real com triggers e alertas automáticos para sistemas críticos, VPN, links, servidores, CPU, memória, disco, serviços e aplicações.	Detecção preventiva ou imediata de indisponibilidade e degradação.
Comitê de gestão de crises	Criar rotina mensal para acompanhamento de riscos, continuidade operacional, melhorias, incidentes, processos e indicadores.	Visibilidade executiva e decisões priorizadas por risco.
Acesso remoto	Evoluir o modelo de VPN/TSplus/telefonia, com redução de redirecionamentos sensíveis e validação de alternativas para VoIP/Discador.	Maior estabilidade para usuários em home office.
Governança de exposição	Revisar periodicamente NATs, serviços publicados, origens permitidas e responsáveis por cada exceção.	Menor superfície de ataque e maior controle operacional.

7. Caminho recomendado

Prazo	Objetivo	Ações
Imediato	Reduzir risco crítico	Revisar FreePBX exposto, CentOS 7 EOL, NATs/publicações e serviços externos de maior risco.
Curto prazo	Estabilizar operação	Avaliar aumento de memória do TSplus para 45 GB, reduzir redirecionamentos RDP e padronizar requisitos de rede home office.
Curto prazo	Separar telefonia	Reavaliar Discador/VoIP dentro do TSplus e buscar alternativa fora da sessão remota ou homologada.
Curto prazo	Proteger CRM Gestão	Tratar falhas do Discador como impacto direto no CRM Gestão, pois afetam atendimento, cobrança e produtividade operacional.
Médio prazo	Fortalecer acesso remoto	Avaliar migração de SSL-VPN para IPsec VPN/ZTNA, revisar políticas de acesso e implementar MFA.
Médio prazo	Melhorar governança	Implementar monitoramento ponta a ponta: VPN, TSplus, cloud, links, memória, disco, RDP e aplicações.
Mensal	Gestão contínua	Realizar comitê de riscos/crises, revisar indicadores, status de correções, patches, incidentes e exposição externa.
Após correções	Validar remediação	Executar nova avaliação de segurança para confirmar mitigação das vulnerabilidades.

8. Ações prioritárias para decisão da FÁCIL

Prioridade	Decisão/Ação
1	Autorizar revisão das publicações/NATs e serviços expostos no firewall local e cloud.
2	Priorizar correção ou substituição do FreePBX exposto e do sistema operacional em fim de vida.
3	Avaliar aumento de memória do servidor TSplus para 45 GB e acompanhar consumo após alteração.
4	Reduzir redirecionamentos sensíveis no TSplus, principalmente áudio, microfone, USB e dispositivos locais.
5	Definir se a telefonia continuará dentro do TSplus ou se será migrada para modelo mais adequado.
6	Reconhecer o impacto do Discador no CRM Gestão e tratar falhas de telefonia como risco operacional.
7	Solicitar relatório de desempenho e banda da Armazém Cloud em janela mínima de 7 dias.
8	Implantar dashboard em tempo real com triggers para sistemas críticos e alertas automáticos.
9	Padronizar automação de patches com periodicidade definida e acompanhamento executivo.
10	Criar Comitê de Gestão de Crises e Melhoria Contínua com revisão mensal dos riscos.

Mensagem final

O ambiente possui base técnica operacional, porém a evolução recomendada é sair de uma atuação reativa para um modelo preventivo: gestão mensal de riscos, monitoramento em tempo real, correção priorizada por criticidade e governança sobre alterações, publicações e continuidade operacional.