Prefeitura Municipal de Ferraz de Vasconcelos

AVALIAÇÃO DE SEGURANÇA DA INFORMAÇÃO

Escopo Técnico para Testes de Intrusão Controlados

Henriky de Sena Rodrigues

18 de junho, 2025

1. Introdução

O presente documento tem por finalidade apresentar o escopo preliminar para a realização de testes de segurança ofensiva, também conhecidos como testes de intrusão (*penetration tests* ou *pentests*), no ambiente digital da Prefeitura Municipal de Ferraz de Vasconcelos. A iniciativa se insere no contexto do processo de transformação digital pelo qual passa a administração pública municipal, o qual tem promovido a digitalização de serviços, a informatização de fluxos administrativos e a ampliação da interoperabilidade entre sistemas.

Neste contexto, a adoção de medidas preventivas e proativas no âmbito da segurança da informação mostra-se essencial para assegurar a resiliência cibernética da Administração Pública Municipal. A realização dos testes propostos tem como objetivo identificar, analisar e relatar vulnerabilidades técnicas que possam comprometer a **integridade**, a **confidencialidade** e a **disponibilidade** das informações institucionais e dos serviços públicos. Tais ações estão em estrita conformidade com os preceitos estabelecidos na **Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD)**, na **Lei nº 12.965/2014 (Marco Civil da Internet)**, na **Instrução Normativa SGD/ME nº 1/2020**, que dispõe sobre a política de segurança da informação nos órgãos e entidades da administração pública, e com as diretrizes técnicas da **norma ABNT NBR ISO/IEC 27001**, que trata dos requisitos para a implementação de um Sistema de Gestão da Segurança da Informação (SGSI).

A execução controlada de testes de intrusão, também denominados **testes de penetração (penetration tests ou pentests)**, constitui prática consolidada e reconhecida, tanto em âmbito nacional quanto internacional, como instrumento eficaz para avaliar a robustez e a resiliência de ativos tecnológicos frente a ameaças reais. Essa metodologia, conduzida de forma ética, controlada e autorizada, visa à simulação de técnicas e táticas comumente utilizadas por agentes maliciosos, com o intuito de evidenciar vulnerabilidades que, se exploradas, poderiam comprometer a confiança da população, a continuidade operacional dos serviços públicos e a conformidade legal da Administração

quanto ao tratamento de dados sensíveis, nos termos das legislações e normas vigentes.

Este escopo preliminar visa orientar a execução dos testes técnicos, definindo os ativos a serem avaliados, os métodos aplicados e os cuidados necessários para garantir a continuidade dos serviços e a proteção dos dados. Trata-se de uma medida estratégica para reforçar a segurança cibernética e assegurar uma gestão pública digital segura, eficiente e alinhada às normas legais vigentes no presente momento.

2. Objetivo Geral

O objetivo geral deste trabalho é avaliar, de forma sistemática e controlada, a resiliência da infraestrutura digital da Prefeitura Municipal de Ferraz de Vasconcelos frente as ameaças cibernéticas contemporâneas. Para tanto, serão realizadas simulações de ataques direcionados com o intuito de identificar vulnerabilidades técnicas, falhas de configuração, deficiências nos procedimentos operacionais e outros pontos de fragilidade que possam ser explorados por agentes mal-intencionados.

Essa avaliação visa não apenas revelar brechas existentes, mas também subsidiar a formulação de recomendações técnicas e administrativas voltadas à mitigação dos riscos identificados, fortalecendo os mecanismos de defesa da organização. Ao final do processo, espera-se oferecer um diagnóstico confiável, embasado nas diretrizes da norma **ISO/IEC 27001**, reconhecida internacionalmente como referência na gestão da segurança da informação.

Além disso, o cumprimento desse objetivo contribuirá diretamente para o aprimoramento da postura de segurança cibernética da Prefeitura, promovendo a continuidade dos serviços públicos digitais, a proteção dos dados sensíveis e a conformidade com os princípios legais estabelecidos pela **Lei Geral de Proteção de Dados Pessoais (LGPD)** e demais normativas aplicáveis ao setor público.

3. Objetivos Específicos

Com base nas diretrizes da norma **ISO/IEC 27001** e nas boas práticas de segurança da informação, este trabalho contempla os seguintes objetivos específicos, que orientarão a execução dos testes de intrusão no ambiente digital da Prefeitura Municipal de Ferraz de Vasconcelos:

- **Mapear vulnerabilidades em aplicações web e serviços internos**, com foco na identificação de falhas de segurança que possam ser exploradas para obtenção de acesso não autorizado, manipulação de dados ou interrupção de serviços. Essa etapa inclui a análise de códigos, configurações e pontos de entrada expostos à internet ou à rede interna.

- **Analisar a estrutura e configuração da rede local (LANs e VLANs)**, a fim de detectar possíveis fragilidades na segmentação, roteamento e isolamento de dispositivos e serviços, considerando riscos de movimentação lateral e escalonamento de privilégios por agentes maliciosos.

- **Identificar fragilidades em dispositivos de rede**, como roteadores, switches, impressoras e outros ativos conectados, avaliando suas configurações de segurança, firmware, exposição de serviços e possíveis falhas de gerenciamento que comprometam a integridade da rede.

- **Verificar a robustez dos mecanismos de autenticação e controle de acesso**, incluindo a análise de políticas de senha, autenticação multifator, permissões de usuários e segregação de privilégios, com o objetivo de garantir que os controles implementados sejam eficazes na prevenção de acessos indevidos.

- **Avaliar práticas de segurança relacionadas ao comportamento humano**, por meio de testes de engenharia social controlados, de forma a mensurar o grau de conscientização dos colaboradores sobre ameaças digitais e

identificar vulnerabilidades ligadas a fatores humanos, como o compartilhamento indevido de credenciais ou o acesso a links maliciosos.

- **Propor melhorias para a governança de segurança da informação e boas práticas**, com recomendações que visem o fortalecimento da estrutura organizacional, definição clara de responsabilidades, criação ou revisão de políticas internas, além da promoção de uma cultura institucional voltada à proteção da informação e à conformidade normativa.

Esses objetivos compõem um conjunto abrangente de ações voltadas à detecção preventiva de riscos, fornecendo subsídios técnicos e estratégicos para a construção de um ambiente digital mais seguro, resiliente e alinhado às exigências legais e normativas aplicáveis à administração pública.

4. Metodologia Adotada

A metodologia adotada para a realização dos testes de intrusão será fundamentada em **frameworks consolidados e reconhecidos internacionalmente**, os quais oferecem abordagens sistemáticas e estruturadas para a condução segura e eficaz de avaliações de segurança ofensiva. Dentre os principais referenciais utilizados destacam-se:

- **OWASP (Open Web Application Security Project)**: iniciativa global que fornece diretrizes atualizadas sobre vulnerabilidades em aplicações web, incluindo o conhecido OWASP Top 10, utilizado como base para identificação de falhas críticas no desenvolvimento e implantação de sistemas web.

- **PTES (Penetration Testing Execution Standard)**: padrão de execução de testes de penetração que orienta as fases do processo, desde o planejamento até a entrega do relatório final, garantindo padronização, clareza metodológica e consistência técnica.

- **MITRE ATT&CK Framework**: base de conhecimento mantida pela MITRE Corporation, que cataloga táticas, técnicas e procedimentos (TTPs) utilizados por invasores servindo como referência para simulações realistas de ataques e para a análise comportamental dos vetores de ameaça.

A execução dos testes seguirá uma **sequência lógica de etapas**, ajustada às particularidades do ambiente da Prefeitura Municipal de Ferraz de Vasconcelos, conforme descrito a seguir:

1. **Coleta de informações (passiva e ativa)**: levantamento de dados públicos e internos que permitam compreender a superfície de ataque, sem causar impactos ao ambiente operacional.

2. **Enumeração de alvos e serviços**: identificação detalhada de dispositivos, portas, serviços e aplicações disponíveis na infraestrutura, com o objetivo de mapear possíveis pontos de entrada.

3. **Análise de vulnerabilidades conhecidas**: investigação técnica dos alvos identificados, utilizando ferramentas automatizadas e análise manual, com foco na detecção de falhas exploráveis.

4. **Execução de exploits controlados**: tentativa de exploração das vulnerabilidades em ambiente autorizado, de forma controlada, segura e documentada, visando comprovar os riscos sem comprometer a estabilidade e integridade dos sistemas.

5. **Elaboração de relatórios técnico e executivo**: consolidação dos achados em dois formatos complementares — um relatório técnico detalhado com evidências, vetores explorados e sugestões de correção, e um relatório executivo com linguagem acessível à alta gestão, destacando os riscos estratégicos e as ações prioritárias.

Essa metodologia assegura a **efetividade, rastreabilidade e integridade do processo**, permitindo que os resultados obtidos sirvam de base confiável para

decisões estratégicas em segurança da informação, sempre em conformidade com os princípios éticos e legais que regem a atuação da administração pública.

5. Escopo Técnico

O escopo técnico deste trabalho contempla uma avaliação detalhada dos ativos digitais e componentes de infraestrutura da Prefeitura Municipal, com foco na identificação de vulnerabilidades e fragilidades que possam comprometer a segurança da informação. As análises serão conduzidas com base em boas práticas reconhecidas, considerando abordagens ofensivas controladas e metodologias consagradas, como o OWASP Top 10 e os padrões do PTES. O escopo está subdividido nos seguintes eixos temáticos:

5.1 Aplicações Web e Sistemas Digitais

Serão conduzidos testes de segurança em aplicações web, com base nos principais riscos descritos pelo **OWASP Top 10**, incluindo injeções (Injection), falhas de autenticação (Broken Authentication), exposição de dados sensíveis (Sensitive Data Exposure), dentre outros. A análise contemplará:

- Verificação de dependências e bibliotecas desatualizadas, que possam representar vetores de ataque exploráveis;
- Tentativas de acesso não autorizado a funcionalidades administrativas ou privilegiadas;
- Testes sobre mecanismos de autenticação, controle de sessões e tratamento de credenciais;
- Simulações de exfiltração de dados sensíveis, de forma controlada, para avaliar a eficácia dos mecanismos de proteção implementados.

5.2 Infraestrutura de Rede

A estrutura de rede da Prefeitura será analisada sob a ótica de sua segmentação, interconectividade e exposição. As atividades incluirão:

- Verificação da segmentação lógica por VLANs e identificação de possíveis falhas em sua implementação;
- Análise dos pontos de interconexão entre redes e possíveis caminhos para saltos entre VLANs;
- Detecção e mapeamento de dispositivos e serviços ativos na rede por meio de varreduras não intrusivas;
- Realização de testes simulados como **ARP spoofing**, **DNS poisoning** e **sniffing**, com o objetivo de evidenciar riscos relacionados à manipulação de tráfego interno.

5.3 Dispositivos de Rede e Compartilhamento

A avaliação se estenderá aos equipamentos de rede e dispositivos de uso compartilhado. Os testes abordarão:

- Análise da segurança de roteadores, switches e impressoras quanto a configurações padrão, acessos administrativos e senhas frágeis;
- Verificação da atualização de firmware e aplicação de correções críticas de segurança;
- Identificação de serviços expostos indevidamente (como Telnet e SNMP);
- Investigação de compartilhamentos públicos de arquivos ou impressoras que possam representar risco de vazamento de informações.

5.4 Senhas e Autenticação

O ambiente será avaliado quanto à robustez dos mecanismos de autenticação e à gestão de credenciais, com foco em:

- Identificação de senhas fracas, reutilizadas ou configuradas com padrões de fábrica;
- Execução de ataques de dicionário e força bruta, sempre em ambiente controlado e com as devidas autorizações;
- Enumeração de usuários válidos e mapeamento de privilégios associados;
- Verificação de contas com permissões excessivas, que possam representar riscos em caso de comprometimento.

5.5 Engenharia Social (com explícito consentimento)

Com o consentimento prévio e o controle adequado dos testes, serão realizadas simulações que buscam mensurar a vulnerabilidade da organização a técnicas de engenharia social, incluindo:

- Execução de campanhas simuladas de **phishing** direcionadas a colaboradores previamente selecionados;
- Tentativas controladas de obtenção de informações sensíveis por meio de abordagens sociais;
- Avaliação da maturidade da cultura organizacional em relação à segurança da informação e boas práticas de conscientização.

5.6 Simulação Ética de Ataques DDoS

Por fim, será avaliada a capacidade da infraestrutura de suportar tentativas de negação de serviço, observando os limites operacionais e as proteções vigentes. As ações previstas incluem:

- Análise de eventuais mecanismos de mitigação disponibilizados pela operadora ou provedor de internet;
- Testes de **stress não disruptivos**, como o envio de múltiplas conexões simultâneas dentro dos limites acordados;
- Recomendações sobre a adoção de soluções técnicas como **CDN (Content Delivery Network)**, **WAF (Web Application Firewall)** e políticas de **rate limiting**, de modo a fortalecer a resiliência contra esse tipo de ameaça.

6. Limitações e Restrições

A execução dos testes de segurança será conduzida com base em critérios técnicos, éticos e operacionais rigorosos, visando preservar a estabilidade do ambiente tecnológico e assegurar a continuidade dos serviços públicos prestados pela Prefeitura Municipal de Ferraz de Vasconcelos. Em nenhuma

hipótese serão realizadas ações que possam resultar em interrupções, danos ou impactos nos sistemas em produção. Todos os procedimentos serão previamente autorizados pelas instâncias gestoras competentes, de forma a garantir a conformidade com as diretrizes institucionais e o pleno alinhamento com os princípios de responsabilidade pública.

Técnicas como engenharia social, análise de autenticação, exploração de vulnerabilidades em aplicações web, testes em dispositivos de rede, simulações de ataques em infraestrutura e demais abordagens previstas neste escopo serão executadas exclusivamente em ambientes controlados, mediante autorização formal e com total observância aos limites acordados. No caso específico de simulações de ataques de negação de serviço distribuída (DDoS), reforça-se que **não será realizado qualquer teste real** que envolva geração de tráfego ou sobrecarga de sistemas. Serão adotadas apenas análises teóricas e avaliações não intrusivas da capacidade de resposta da infraestrutura frente a esse tipo de ameaça.

Essa abordagem visa garantir que todo o processo ocorra com total responsabilidade técnica, minimizando riscos operacionais e reforçando o compromisso institucional com a segurança da informação, a transparência e a prestação contínua e eficaz dos serviços públicos à população.

7. Entregáveis

Ao término das atividades de avaliação, serão produzidos e entregues documentos técnicos e gerenciais que subsidiarão a tomada de decisão estratégica por parte da administração pública municipal. O principal produto será um **relatório técnico detalhado**, contendo as ferramentas que foram utilizadas, a descrição das vulnerabilidades identificadas durante os testes, acompanhadas de evidências técnicas, análise dos impactos potenciais e recomendações corretivas específicas, classificadas conforme o nível de criticidade.

Complementarmente, será elaborado um **relatório executivo**, direcionado às lideranças da gestão pública, com linguagem acessível e objetiva, no qual serão destacados os riscos mais relevantes, de modo a facilitar o entendimento não técnico e fomentar ações corretivas em nível administrativo e decisório.

Também será apresentado um **Plano de Ação Prioritário**, com sugestões de correção organizadas conforme a severidade das vulnerabilidades encontradas e o potencial impacto sobre os ativos da Prefeitura, permitindo a definição de uma agenda estratégica de mitigação de riscos. Por fim, serão incluídas recomendações de boas práticas e diretrizes de governança em segurança da informação, com o objetivo de fortalecer a postura institucional frente as ameaças cibernéticas, em conformidade com os marcos legais vigentes e as normas internacionais aplicáveis.

8. Considerações Finais

Este escopo reafirma o compromisso da Prefeitura Municipal de Ferraz de Vasconcelos com a segurança e a integridade de sua infraestrutura tecnológica, ressaltando a importância de assegurar a integridade dos ativos digitais diante dos desafios contemporâneos da segurança cibernética. A contínua modernização dos processos administrativos é essencial para a eficiência da gestão pública e para a melhoria dos serviços prestados à população, sendo dever da Prefeitura garantir um ambiente digital seguro, resiliente e confiável.

O presente trabalho encontra-se embasado no ordenamento jurídico brasileiro, com ênfase em dispositivos legais considerados essenciais à salvaguarda da segurança da informação no âmbito da administração pública, entre as quais se destacam a Lei nº 13.709/2018 — Lei Geral de Proteção de Dados Pessoais (LGPD) — que estabelece diretrizes para o tratamento adequado e seguro de dados pessoais; e a Lei nº 12.737/2012 — conhecida como Lei Carolina Dieckmann — que tipifica como crime a invasão de dispositivos eletrônicos, tais como computadores e celulares, com a finalidade de obter, adulterar ou destruir dados ou informações sem autorização. Essa lei também criminaliza a

divulgação não autorizada de informações íntimas, reforçando a proteção da privacidade e da dignidade dos munícipes. Além disso, observa-se plena conformidade com normas internacionais de referência, especialmente a ISO/IEC 27001, que define os requisitos para a implementação e manutenção de sistemas de gestão de segurança da informação.

Assim, este escopo não se limita à identificação de vulnerabilidades e mitigação de riscos, mas se consolida como uma iniciativa estratégica voltada à promoção de uma cultura organizacional sólida em segurança da informação, alinhada às especificidades da administração pública e às exigências legais e normativas vigentes. A proteção de dados sensíveis e a continuidade dos serviços públicos são obrigações fundamentais da gestão municipal, diretamente relacionadas à preservação da confiança da população nas instituições públicas.

Nesse sentido, a transformação digital em curso na Prefeitura Municipal de Ferraz de Vasconcelos deve ser conduzida de forma planejada, segura e sustentável, em conformidade com as leis aqui descritas e com os parâmetros estabelecidos por normas técnicas como a ABNT NBR ISO/IEC 27001, garantindo a **integridade**, a **disponibilidade** e a **confidencialidade** das informações sob sua responsabilidade.

9. Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27001:2013**. *Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos.* Rio de Janeiro: ABNT, 2013.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012.** *Tipifica crimes informáticos e altera o Código Penal.* Diário Oficial da União: seção 1, Brasília, DF, 3 dez. 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 18 jun. 2025.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** *Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.* Diário Oficial da União: seção 1, Brasília, DF, ano 151, n. 77, p. 1, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 18 jun. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. *Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Lei Geral de Proteção de Dados – LGPD).* Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 18 jun. 2025.

BRASIL. **Ministério da Economia. Secretaria de Governo Digital. Instrução Normativa SGD/ME nº 1, de 27 de maio de 2020.** *Dispõe sobre as ações de segurança da informação e comunicações no âmbito da administração pública federal, direta, autárquica e fundacional.* Diário Oficial da União: seção 1, Brasília, DF, p. 12, 28 maio 2020. Disponível em: https://www.in.gov.br/en/web/dou/-/instrucao-normativa-sgd/me-n-1-de-27-de-maio-de-2020-258003368. Acesso em: 18 jun. 2025.

OPEN WEB APPLICATION SECURITY PROJECT. *OWASP Top Ten – 2021: The Ten Most Critical Web Application Security Risks.* OWASP Foundation, 2021. Disponível em: https://owasp.org/Top10. Acesso em: 18 jun. 2025.