Universidade de Brasília

departamento de engenharia elétrica

Gestão e segurança para contas de usuários no Active Directory

ALUNO(S)/MATRÍCULA(S): **Rodrigo Poubel dos Santos / 241203616**

ORIENTADOR: João Souza Neto, Dr.

Abstract: O Active Directory (AD) é uma plataforma essencial para a administração de redes corporativas, oferecendo uma solução centralizada para o gerenciamento de identidades, autenticação e controle de acesso a recursos. À medida que as organizações se tornam cada vez mais dependentes de sistemas interconectados, a segurança do AD se torna um aspecto crítico para proteger dados sensíveis e garantir a integridade da infraestrutura de TI. Este estudo explora as melhorias que podem ser implementadas por meio de políticas de segurança, configurações de segurança aprimoradas e práticas de controle de acesso, capazes de minimizar as vulnerabilidades, prevenir acessos não autorizados e fortalecer a proteção contra ameaças cibernéticas que vão desde ataques de escalonamento de privilégios, técnicas de autenticação maliciosa e exploração de credenciais comprometidas. A metodologia empregada teve uma abordagem descritiva, utilizando ferramentas de auditoria em ambientes controlados e análise de relatórios. Foi desenvolvido um estudo de caso em uma rede simulada para identificar e avaliar potenciais falhas de segurança como configurações inadequadas, ataques internos e externos, e o uso de credenciais comprometidas. A partir dos dados obtidos, foi possível elaborar recomendações práticas para mitigação dos riscos como a implementação de políticas rigorosas de controle de acesso, auditorias periódicas e o uso de ferramentas de monitoramento contínuo. O estudo também contribui para o avanço do conhecimento sobre as melhores práticas de configuração e gestão do Active Directory, fornecendo um referencial teórico e prático para organizações que buscam fortalecer sua segurança cibernética. Essas contribuições são relevantes para profissionais de TI, principalmente da área da segurança da informação, visando a construção de ambientes mais seguros e resilientes.

Palavras-chave – Active Directory, Gerenciamento de Contas, Proteção de Identidades, Mitigação de Vulnerabilidades, Controle de Acesso, Gestão de Riscos, Segurança da Informação.

1. INTRODUÇÃO

A crescente dependência das organizações dos sistemas de informação torna a segurança da informação um fator essencial para a continuidade dos negócios e a proteção de dados sensíveis. Nesse cenário, proteger os ambientes tecnológicos contra ameaças internas e externas tornou-se uma exigência estratégica, visando garantir a confidencialidade, integridade e disponibilidade das informações por meio da aplicação de controles e avaliação de riscos.

O Active Directory (AD), solução da Microsoft amplamente adotada para o gerenciamento centralizado de identidades, autenticação e controle de acesso, desempenha papel crítico nas infraestruturas corporativas modernas. Por concentrar informações sensíveis sobre contas de usuários, permissões e recursos de rede, o AD torna-se não apenas um recurso vital, mas também um alvo estratégico para agentes maliciosos. Qualquer falha em sua segurança pode levar ao comprometimento total do ambiente, permitindo, por exemplo, a elevação de privilégios e o controle indevido de ativos corporativos (MICROSOFT, 2025).

Sob a perspectiva da ISO 31000, risco é definido como o “efeito da incerteza sobre os objetivos”, sendo fundamental que as organizações adotem uma abordagem estruturada para a identificação, análise, avaliação, tratamento e monitoramento de riscos (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2018). A aplicação dessa norma à administração do Active Directory

permite reduzir impactos associados a falhas técnicas, erros humanos ou acessos indevidos, fortalecendo a postura de segurança e aumentando a resiliência da organização frente a eventos inesperados.

O AD também desempenha um papel importante proporcionando uma plataforma para integração de soluções de terceiros e sistemas corporativos. Sua implementação facilita a interoperabilidade entre diferentes sistemas operacionais e plataformas, uma vez que ele pode ser configurado para trabalhar com protocolos padrões, como LDAP (Ligthweight Directory Access Protocol), DNS (*Domain Name System*) e Kerberos.

Porém, a gestão do AD exige cuidados e práticas adequadas, pois sua falha ou má configuração podem comprometer toda a segurança e operação da rede corporativa. Questões como a replicação de dados, gestão de identidade, controle de acesso e segurança são fundamentais para a manutenção da integridade e da confiança no sistema.

Diante disso, este artigo tem como objetivo analisar o Active Directory sob a ótica da gestão de riscos e de segurança, evidenciando como as normas internacionais contribuem para a proteção de identidades digitais, a mitigação de vulnerabilidades e a consolidação da segurança da informação nas organizações.

2. REFERENCIAL TEÓRICO

Nesta seção são apresentados os conceitos do Active Directory e do Processo de Gestão de Riscos (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2018).

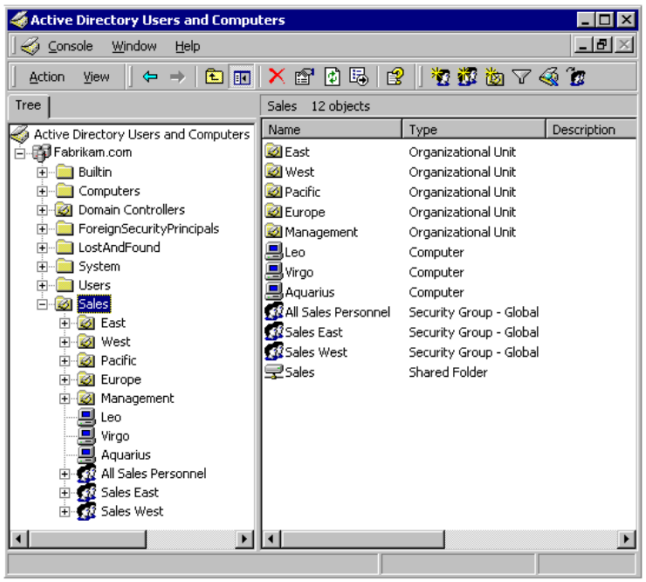
2.1 ACTIVE DIRECTORY

2.1.1. CONCEITO

O Active Directory (AD) é um serviço de diretório cuja principal função é realizar o gerenciamento centralizado de identidades, recursos e políticas de segurança em redes corporativas baseadas no sistema operacional Windows Server. Ele permite que administradores controlem a autenticação de usuários, permissões de acesso e configurações de dispositivos de forma hierárquica e padronizada (MICROSOFT, 2025).

O AD armazena objetos como usuários, grupos, computadores e unidades organizacionais (OUs) e opera por meio de um ou mais controladores de domínio, responsáveis por autenticar usuários, aplicar regras de segurança (Group Policy Object - GPO) e garantir a integridade das informações replicadas em toda a rede (NIST, 2017). O domínio é a unidade básica da organização lógica no Active Directory. Ele agrupa objetos como usuários, computadores, grupos e impressoras sob uma mesma base de dados e políticas de segurança. Cada domínio é identificado por um nome DNS exclusivo, como nome do dominio.local, e é gerenciado por um ou mais controladores de domínio (Domain Controllers). A figura 1 ilustra essa organização.

Figura 1: Usuários e computadores no Active Directory



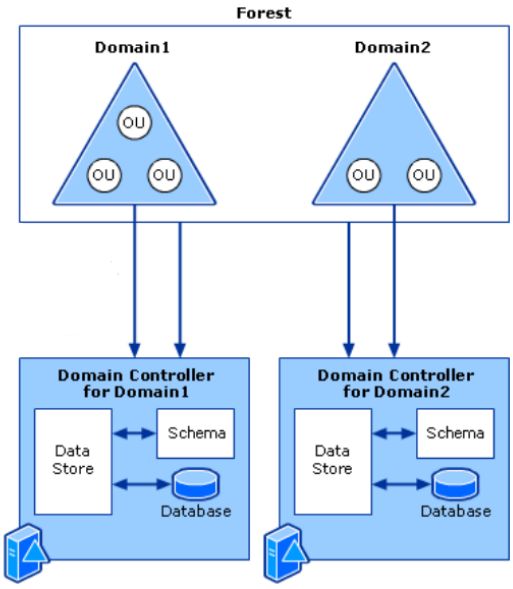
Fonte: Microsoft (https://learn.microsoft.com/pt-br/windows/win32/adsi/so-what-is-active-directory) acessado em 03/03/2025

Segundo a Microsoft (2023), os domínios permitem que administradores apliquem regras específicas, segmentem acessos e definam permissões com base em regras organizacionais. Eles representam limites de segurança, replicação e gerenciamento.

Uma floresta (forest) é o nível mais alto da estrutura lógica do Active Directory. Ela representa um conjunto de um ou mais domínios que compartilham uma configuração comum, incluindo o esquema do diretório (definição de objetos e atributos) e o catálogo global. Dentro de uma floresta, os domínios mantêm relações de confiança transversais e transitivas por padrão,

possibilitando autenticação entre eles. A floresta é considerada o limite máximo de segurança no AD. A figura 2 ilustra o conceito de floresta.

Figura 2: Active Directory Data Structure and Storage



Fonte: Microsoft (https://learn.microsoft.com/pt-br/previous-versions/windows/it-pro/windows-server-2003/cc759186(v=ws.10)) acessado em 03/03/2025

2.1.2 FUNCIONALIDADES

Em uma infraestrutura baseada no Active Directory, a replicação e a atualização de dados ocorrem de forma multimestre entre controladores de domínio. No entanto, certas tarefas críticas requerem um controle centralizado para evitar conflitos ou inconsistências. Para isso, o AD define cinco funções Flexible Single Master Operations (FSMO).

Essas funções são atribuídas a controladores de domínio específicos, que atuam como mestres exclusivos para determinadas operações. O gerenciamento correto dessas funções é essencial para a estabilidade, integridade e segurança da estrutura do AD (MICROSOFT, 2023).

As funções FSMO são divididas em dois grupos (Florestas e domínios).

Em nível de floresta, temos:

- Schema Master (responsável por atualizar o esquema do AD, ou seja, a definição dos tipos de objetos e atributos);

- Domain Naming Master (controla a adição e remoção de domínios na floresta, bem como garante a unicidade dos nomes de domínio).

Em nível de domínio, temos:

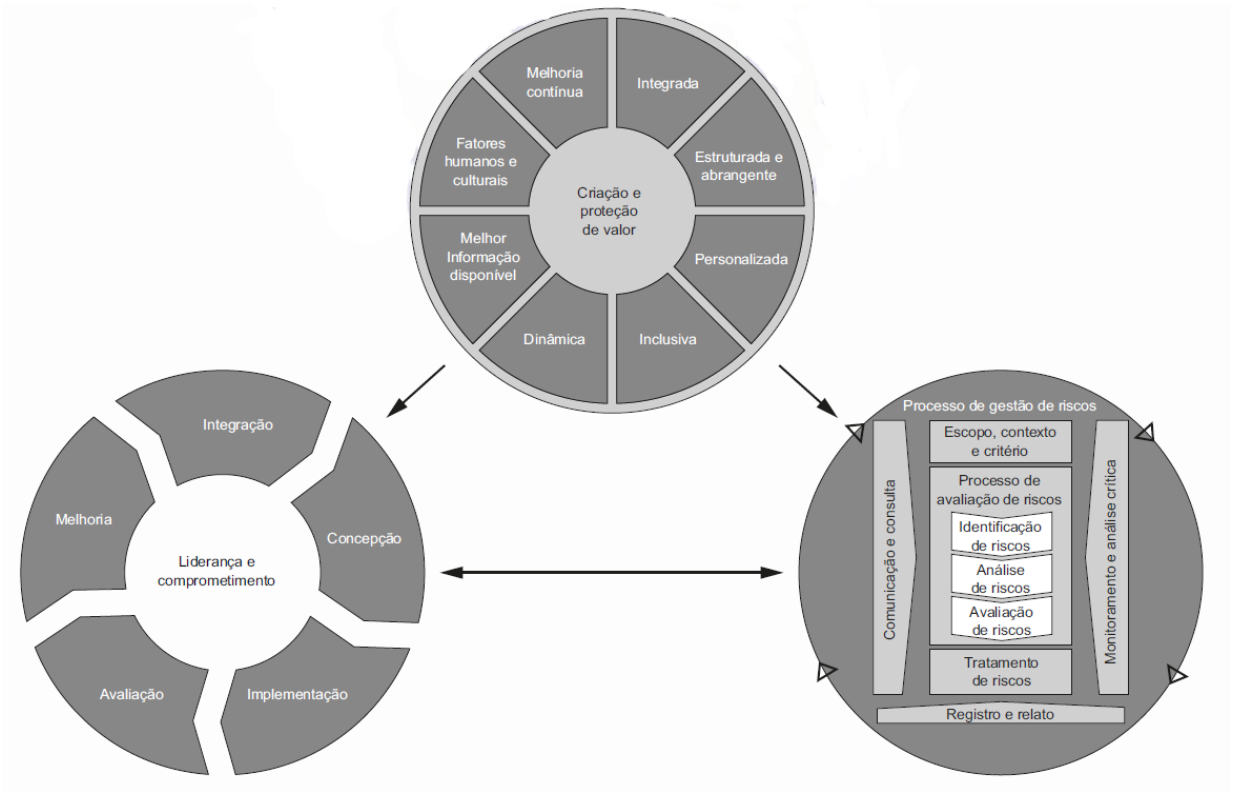
- RID Master, responsável por distribuir blocos de Identificadores Relativos (RIDs) aos DCs do domínio e garantir que cada objeto criado no AD tenha um identificador único;
- PDC Emulator. Atua como servidor de hora (NTP) do domínio. É o responsável por autenticação legada, políticas de senha e suporte a alterações imediatas de senha. É crucial para compatibilidade com versões antigas do Windows e replicações urgentes;
- Infrastructure Master. Atualiza referências cruzadas entre objetos de domínios diferentes.

Portanto, o AD tem um papel importante na gestão centralizada de identidades e acessos, permitindo o controle eficiente de recursos, a aplicação de políticas de segurança e a mitigação de riscos em ambientes corporativos.

2.1 GESTÃO DE RISCOS (ABNT NBR ISO 31000)

A ISO 31000 é uma norma internacional que fornece diretrizes para a gestão de riscos em qualquer tipo de organização. Ela estabelece uma abordagem estruturada e personalizada para identificar, analisar, avaliar, tratar, monitorar e comunicar riscos, promovendo a tomada de decisões baseada em evidências e a melhoria contínua dos processos organizacionais (ISO, 2018). A norma ISO 31000 estabelece diretrizes para a gestão de riscos organizacionais, fundamentando-se em três componentes principais: princípios, estrutura e processo. Os princípios orientam a eficácia da gestão de riscos, destacando a integração com os processos organizacionais, a base para tomada de decisão, a transparência e a melhoria contínua. A estrutura define como a gestão de riscos deve ser incorporada à governança e à cultura da organização, estabelecendo papéis, responsabilidades, recursos e comunicação. Por fim, o processo de gestão de riscos é cíclico e composto pelas etapas de comunicação e consulta, estabelecimento do contexto, identificação, análise e avaliação dos riscos, tratamento, além do monitoramento e revisão. Essa abordagem sistemática contribui para a criação de valor, a proteção de ativos e o alcance dos objetivos organizacionais em ambientes incertos (ISO, 2018). A figura 3 apresenta os três componentes.

Figura 3: Estrutura, princípio e processo



Fonte: ABNT ABR ISO 31000

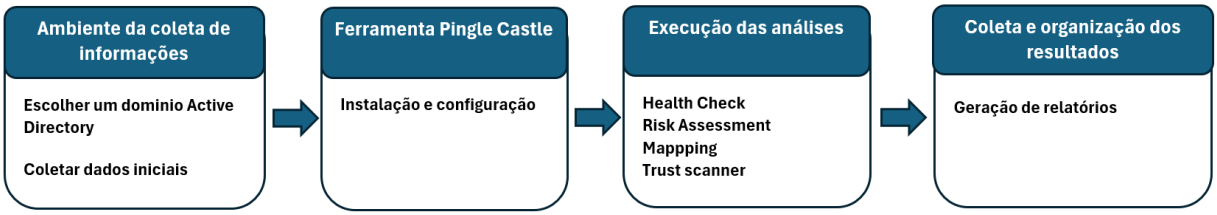
A ISO 31000 oferece uma base robusta, adaptável e integrada para a gestão de riscos em organizações de todos os setores. Ao ser aplicada em conjunto com frameworks técnicos como o Active Directory e normas como a ISO/IEC 27001, permite tomadas de decisão mais seguras, melhoria da resiliência cibernética e a prevenção de impactos negativos sobre os objetivos da organização.

3. METODOLOGIA

Esta seção, caracteriza-se como um estudo de caso, de abordagem qualitativa e exploratória, com o objetivo de avaliar os riscos associados à infraestrutura do Active Directory em ambiente

corporativo, por meio do levantamento de vulnerabilidades e de entrevista. A figura 4 ilustra as etapas desse processo.

Figura 4: Etapas do levantamento de vulnerabilidades



Fonte: Autoria própria

3.1 AMBIENTE DA COLETA DE INFORMAÇÕES

A coleta de dados foi realizada em um ambiente configurado com vários controladores de domínio Active Directory on-premises, contendo um domínio. Foi feito o uso da ferramenta Ping Castle, reconhecida por sua capacidade de realizar auditorias rápidas e abrangentes no AD (Martel, 2021).

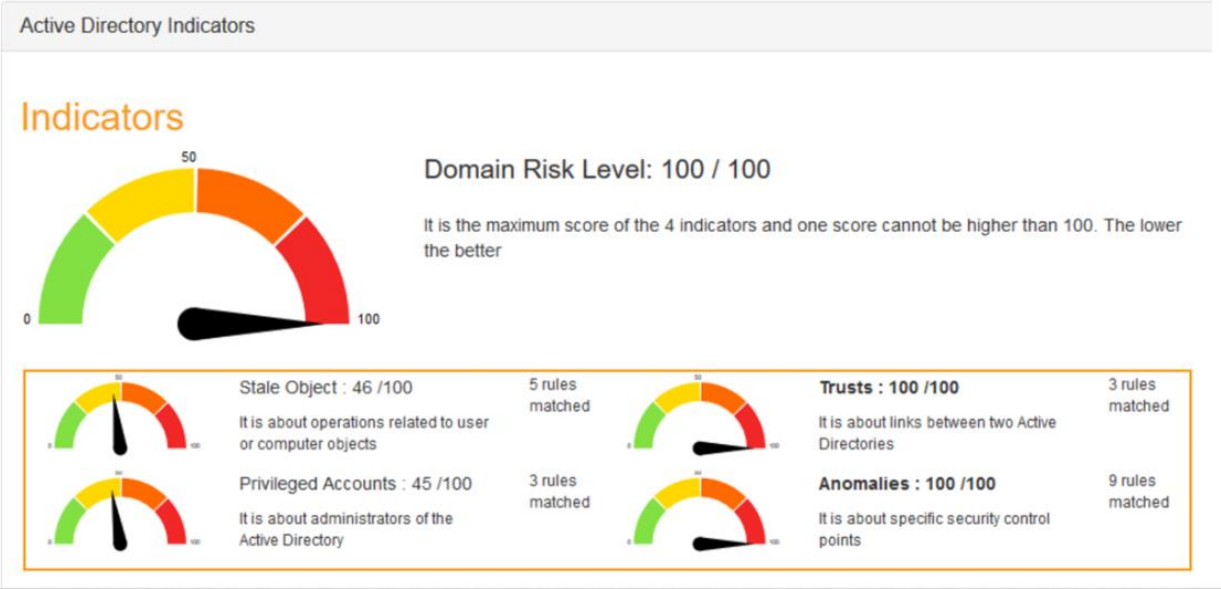
Essa etapa nos permite entender como o AD está configurado e quais as possíveis vulnerabilidades que podem existir (MICROSOST, 2023). A identificação precisa da infraestrutura permite detectar anomalias, delegações excessivas de privilégios e eventuais fragilidades estruturais (CIS, 2021).

3.2 FERRAMENTA UTILIZADA

Para a identificação e análise de riscos associados à infraestrutura do Active Directory, foi escolhida a ferramenta Ping Castle, que se mostrou alinhada aos princípios da norma ISO 31000, voltada à gestão de riscos e apresenta robustez, gratuidade e reconhecimento no mercado de segurança da informação para avaliações de AD. A ferramenta permite uma abordagem sistemática para identificação de vulnerabilidades que podem comprometer a confidencialidade, integridade e disponibilidade do ambiente de AD, pilares fundamentais na gestão de riscos de segurança da informação. De acordo com Schroeder, Barnum e Scott (2022), ferramentas de análise como o Ping Castle auxiliam para mapear caminhos de ataque e apoiar decisões estratégicas na proteção de diretórios corporativos.

O Ping Castle realiza auditorias automatizadas e detalhadas sobre a estrutura do domínio, detectando riscos como contas com privilégios excessivos, senhas fracas, objetos legados e configurações inseguras (PING CASTLE, 2025). A principal funcionalidade empregada nesta pesquisa foi o modo "Health Check", que gera um relatório técnico com um “Health Score”, representando o nível de exposição da organização a riscos de segurança. A figura 5 ilustra os indicadores.

Figura 5: Indicadores dos riscos na ferramenta



Fonte: PingleCastle (https://www.Ping Castle.com/documentation/healthcheck/) acessada em 04/04/2025

3.3 EXECUÇÃO DA ANÁLISE DE SEGURANÇA

A execução da análise foi organizada em quatro módulos principais oferecidos pela ferramenta Ping Castle, cada um com objetivos específicos e procedimentos detalhados.

O primeiro módulo, denominado Health Check, tem como propósito avaliar a integridade geral do ambiente Active Directory. Esta etapa permite identificar configurações obsoletas, objetos inativos, contas privilegiadas sem as proteções adequadas, políticas de senha inconsistentes e outros fatores que comprometem a postura de segurança do domínio. Conforme salientado por Silva (2021), “a verificação de saúde de um Active Directory é o primeiro passo para detectar fragilidades estruturais que podem ser exploradas em ataques avançados”. O Health Check forneceu um índice percentual de saúde do ambiente, servindo como métrica inicial para o estado de segurança observado.

Em seguida, foi realizado o Risk Assessment, uma avaliação focada na detecção de riscos críticos e vulnerabilidades específicas. Essa etapa identificou ameaças como a presença de contas privilegiadas ocultas (Shadow Admins), delegações de privilégios inseguras (Kerberos Delegation Abuse), falhas de configuração em trusts entre domínios e configurações que poderiam permitir o escalonamento de privilégios. De acordo com Martins (2020), "a identificação proativa de riscos críticos no Active Directory é essencial para interromper possíveis cadeias de ataque antes que sejam iniciadas". Além disso, Costa (2019) reforça que “sem uma avaliação rigorosa dos riscos, organizações operam na ilusão de segurança, enquanto vulnerabilidades fundamentais permanecem ativas”, evidenciando a importância desta etapa.

O terceiro módulo, denominado Mapping, consistiu na construção de um mapeamento visual e lógico do ambiente. A ferramenta gerou diagramas que mostraram como os privilégios se propagam entre contas, grupos e unidades organizacionais. Esse mapeamento é considerado estratégico, pois, como observa Almeida (2022), "mapear as relações de privilégios dentro do Active Directory é como traçar o mapa de uma fortaleza: quem conhece os caminhos internos conhece também seus pontos fracos". Gonçalves (2021) complementa: "a movimentação lateral no AD depende da existência de caminhos privilegiados; mapear esses caminhos é prevenir o avanço de invasores".

Por fim, utilizou-se o Scanner de Trusts para avaliar relações de confiança existentes com outros domínios ou florestas. Esta análise permitiu identificar possíveis vulnerabilidades nas trusts configuradas, como a ausência de autenticação adequada ou permissões excessivas concedidas a domínios externos. Moura (2020) alerta que "relações de confiança mal configuradas entre domínios são brechas silenciosas que podem comprometer a segurança de toda a floresta", enquanto Pereira (2023) enfatiza que “o scanner de trusts revela vulnerabilidades não apenas técnicas, mas também administrativas, fruto de práticas inadequadas de gestão de identidades”.

Cada uma dessas análises gerou relatórios detalhados, com evidências, classificações de risco e recomendações de mitigação. Como aponta Santos (2022), “ferramentas como o Ping Castle permitem traduzir ambientes complexos de Active Directory em relatórios acionáveis, democratizando a segurança cibernética para organizações de todos os tamanhos”, destacando a relevância do uso dessa ferramenta no contexto desta pesquisa.

3.4 COLETA E ORGANIZAÇÃO DOS RESULTADOS

A avaliação dos dados coletados a partir das análises do Ping Castle foi estruturada em dois eixos principais: análise quantitativa e análise qualitativa, conforme as boas práticas recomendadas em estudos de segurança da informação.

A análise quantitativa consistiu na mensuração do número de vulnerabilidades identificadas em cada categoria de risco. Cada vulnerabilidade detectada foi classificada com base no seu nível de severidade (baixa, moderada, alta ou crítica), permitindo a construção de um panorama estatístico do estado de segurança do Active Directory. Segundo Oliveira (2021), “a quantificação precisa de vulnerabilidades é fundamental para estabelecer prioridades de correção em ambientes corporativos complexos”. Assim, tabelas e gráficos foram utilizados para organizar visualmente os dados, facilitando a interpretação e a identificação de padrões críticos de exposição.

Em paralelo, foi realizada a análise qualitativa, focada na interpretação do impacto potencial de cada vulnerabilidade detectada. Para essa avaliação, foram considerados aspectos como a facilidade de exploração, o impacto em confidencialidade, integridade e disponibilidade, além das dependências com outros controles de segurança existentes. De acordo com Ferreira (2022), “uma vulnerabilidade tecnicamente simples pode gerar um impacto devastador se explorada em um contexto de má configuração geral”, o que justifica a importância da avaliação qualitativa.

Os critérios de impacto foram baseados nos princípios de gestão de riscos definidos pelas normas ISO/IEC 27005 e NIST SP 800-30, adotando uma perspectiva contextualizada para o ambiente analisado. Complementarmente, foi utilizada a metodologia de priorização por criticidade, como proposto por Souza (2020), que destaca que “a priorização baseada em criticidade é essencial para otimizar recursos e garantir resposta rápida às ameaças mais graves”.

Os dados, após analisados, foram interpretados sob uma ótica de risco residual, considerando o ambiente real de produção e as medidas de segurança já implementadas. Em conformidade com Lima (2021), “a análise de riscos em sistemas de identidade deve sempre considerar o risco residual para que os gestores tenham uma visão fiel das ameaças ativas”.

Esta metodologia garantiu que a avaliação dos resultados fosse tanto abrangente quanto aderente aos padrões de melhores práticas em segurança da informação.

3.5 ANÁLISE DE PERCEPÇÕES PROFISSIONAIS SOBRE DESAFIOS NA SEGURANÇA DO ACTIVE DIRECTORY

Como parte do presente estudo, foi conduzido um levantamento de opinião junto à comunidade profissional por meio da plataforma LinkedIn, com o objetivo de identificar, de forma qualitativa, as percepções mais recorrentes sobre os principais desafios relacionados à segurança do Active Directory no ambiente corporativo. A pergunta formulada foi "Na sua opinião, qual é o maior desafio na segurança do AD?", tendo como respostas as seguintes opções:

a) Detectar contas comprometidas;
b) Controlar privilégios excessivo;
c) Monitorar atividades suspeitas;
d) Aplicar atualizações/hardening.

4. RESULTADOS DO ESTUDO DE CASO E DA ENQUETE

A aplicação da ferramenta para analisar um determinando ambiente corporativo revelou um cenário preocupante de exposição a riscos no Active Directory resultando em um diagnóstico detalhado sobre a superfície de ataque e as vulnerabilidades presentes no ambiente (Metcalf & Nelson, 2022). Dentre os principais resultados foram encontrados:

1. **Identificação de Vulnerabilidades Críticas**

   A ferramenta identificou vulnerabilidades críticas relacionadas a configurações inadequadas de contas privilegiadas, como:

   - Contas com senhas expiradas ou que não exigem troca de senha (Sullivan et al., 2023).
   - Múltiplas contas com privilégios excessivos atribuídos sem necessidade operacional, cenário frequentemente explorado por agentes maliciosos em campanhas de comprometimento (Aleroud & Zhou, 2023).
   - Variável de ambiente chamada "ms-DS-MachineAccountQuota" com a configuração padrão onde é permitido o ingresso de 10 máquinas no domínio por usuário comum (MICROSOFT, 2025).

2. **Avaliação de Conformidade com Boas Práticas**
   A ferramenta forneceu uma pontuação de risco baseada nas práticas recomendadas para o gerenciamento do Active Directory. A média de conformidade antes da implementação de correções foi inferior ao recomendado, indicando a necessidade de ajustes imediatos para alinhar o ambiente às melhores práticas de segurança cibernética (Ferreira & Mattos, 2022).

3. **Relatório de Configurações Obsoletas e Riscos Associados**
   Foram detectadas configurações legadas e práticas obsoletas que expõem o ambiente a ameaças, incluindo:
   - Uso de algoritmos de hash inseguros para senhas, como NTLM (NT LAN Manager) e LM (LAN Manager), os quais permanecem como um vetor clássico de ataques em ambientes corporativos (Hohman, 2023);
   - Presença de controladores de domínio com sistemas operacionais desatualizados, um risco frequentemente associado à manutenção ineficiente da infraestrutura (Aleroud & Zhou, 2023).

Na enquete do linkedin, os resultados demonstraram uma predominância da preocupação com a "Controlar privilégios excessivos" e "monitorar as atividades suspeitas", que obtiveram 33% dos votos cada uma. Isso alerta sobre o risco de acessos privilegiados mal gerenciados em ambientes corporativos e a dificuldade de aplicar estratégias eficazes de *threat hunting* e análise comportamental.
As opções "Detectar contas comprometidas" (22%) e "Aplicar atualizações /hardening" (11%) também foram citadas como desafios relevantes, especialmente em organizações com ambientes híbridos ou históricos de integração de domínios antigos. Todos os participantes são profissionais da área de Segurança da Informação.

5. DISCUSSÃO

A análise das principais vulnerabilidades presentes no Active Directory (AD) evidencia que sua criticidade decorre tanto da centralização dos serviços de autenticação e autorização quanto da sua ampla utilização nas organizações. Ferramentas amplamente difundidas, como Mimikatz,

BloodHound e Impacket, exploram técnicas ofensivas como Pass-the-Hash (PtH), Pass-the-Ticket (PtT), Kerberoasting Golden Ticket, e DCShadow, permitindo que atacantes obtenham controle total do domínio a partir de credenciais comprometidas (SCOTT; METCALF; RYAN, 2022).

Conforme a Microsoft (2023), grande parte das vulnerabilidades exploradas em ambientes AD não resulta de falhas na tecnologia, mas sim da ausência de boas práticas de configuração, gestão de identidades e aplicação de controles de segurança. Esse fato corrobora o entendimento de que a proteção do AD é, antes de tudo, um desafio de governança, gestão de identidade e controle de privilégios.

Uma das estratégias mais efetivas, conforme preconiza a própria Microsoft (2023), é a adoção do modelo de Administração em Camadas (Tiered Administration), que segmenta as credenciais administrativas em diferentes níveis, isolando controladores de domínio, servidores e estações de trabalho. Essa abordagem reduz significativamente a superfície de ataque e impede movimentos laterais em caso de comprometimento de uma conta.

Além disso, práticas como o uso do Princípio do Menor Privilégio, a implementação do Local Administrator Password Solution (LAPS) e o bloqueio de delegações inseguras contribuem diretamente para a redução dos riscos associados ao abuso de credenciais locais e administrativas (KIRKLAND; MARTIN, 2021).

O uso de ferramentas de monitoramento e auditoria fortalece a capacidade das organizações em detectar atividades suspeitas, identificar configurações inseguras e responder de maneira proativa a ameaças (PFEIFFER, 2023). Segundo Scott, Metcalf e Ryan (2022), a visibilidade dos relacionamentos de confiança e a análise das rotas de ataque dentro do AD são fundamentais para antecipar e bloquear possíveis vetores de exploração.

Contudo, embora o uso de Autenticação Multifator (MFA) seja amplamente recomendado, especialmente para contas privilegiadas, este controle isolado não oferece proteção absoluta. A literatura técnica e os padrões de segurança indicam que a segurança do Active Directory deve ser baseada em uma abordagem de defesa em profundidade, que combine controles técnicos, administrativos e operacionais (NIST, 2020; ISO, 2022; CENTER FOR INTERNET SECURITY, 2021).

Portanto, mitigar as vulnerabilidades no Active Directory deve ser encarado como um processo contínuo, incorporado à gestão de riscos da organização, e não como uma ação pontual. Organizações que negligenciam esses princípios permanecem altamente expostas a ataques que

podem comprometer toda a sua infraestrutura tecnológica, resultando em perdas financeiras, operacionais e de reputação (TARANTINO, 2008).

5.1 AS MAIS FREQUENTES VULNERABILIDADES DO ACTIVE DIRECTORY

A análise dos principais ataques ao Active Directory (AD) demonstra que a maioria das vulnerabilidades exploradas está relacionada a configurações inadequadas, gestão deficiente de credenciais e falta de segmentação adequada (Wright, 2021). Isso reflete uma realidade onde, embora as tecnologias estejam maduras, as falhas humanas e operacionais continuam sendo os principais facilitadores dos ataques.

O ataque Golden Ticket permanece como uma das ameaças mais críticas ao AD. Segundo Grassi et al. (2020), este ataque permite que um invasor gere tickets Kerberos falsificados usando o hash da conta KRBTGT, obtendo controle total sobre o domínio. Os autores destacam que uma das principais formas de mitigação é a rotação periódica da chave KRBTGT, além da aplicação rigorosa de MFA e de monitoramento contínuo dos Controladores de Domínio.

No contexto do DCShadow, pesquisa conduzida por Delpy e Lyons (2018) mostra que esse vetor permite que invasores introduzam um controlador de domínio falso para realizar alterações diretamente na base do AD, contornando os mecanismos tradicionais de auditoria. Isso evidencia a importância de limitar rigorosamente as permissões de administradores e de utilizar ferramentas modernas de detecção.

O ataque DCSync permite que adversários abusem de permissões de replicação para obter hashes de senhas diretamente do AD (Spector, 2022). Como defendido por Harman (2020), mitigar este ataque exige uma revisão criteriosa das permissões atribuídas a contas e grupos, principalmente garantindo que apenas os Controladores de Dominios e contas extremamente críticas possuam permissões de replicação.

Entre os ataques de alta criticidade, temos o Pass-the-Hash (PtH) que de acordo com Altherr et al. (2021), ele ocorre quando um invasor usa o hash NTLM para autenticar sem precisar da senha em texto claro. As boas práticas recomendam incluir a desativação do protocolo NTLM, aplicação de Local Administrator Password Solution (LAPS) e implementação de administração escalonada (Tiered Administration).

O Kerberoasting, como destacado por Baggett et al. (2021), explora a má gestão de contas de serviço, permitindo que adversários solicitem tickets de serviço Kerberos e tentem quebrar senhas

offline. Isso reforça a necessidade de senhas fortes, rotação periódica e princípios de privilégio mínimo.

Os ataques NTLM Relay seguem sendo uma ameaça relevante, principalmente em ambientes que ainda mantêm NTLM ativo. De acordo com Zeltser (2021), evitar o uso desse protocolo eliminaria o risco desse ataque.

Outro vetor recorrente é o Credential Dumping, em que atacantes extraem credenciais diretamente da memória (LSASS). Tal como argumentam Forshaw e Howlett (2020), proteger o LSASS com técnicas como RunAsPPL e implementar Credential Guard são práticas indispensáveis para mitigar este risco.

Por fim, as falhas relacionadas ao escalonamento de privilégios via ACLs e DACLs mal configuradas são, segundo Robb (2021), uma das maiores causas de movimentos laterais dentro de ambientes AD.

Esses ataques reforçam a necessidade de um modelo de segurança baseado no conceito de Zero Trust, aliado ao monitoramento contínuo e à adoção de controles proativos de detecção e resposta, como sugerem Kindervag (2010) e Wright (2021). Na tabela 1, resumimos os tipos de ataques e a mitigação para cada um deles:

Tabela 1: Vulnerabilidades e mitigação

Tipo de Ataque	Nível de Criticidade	Explicação do Ataque	Como Mitigar
Golden Ticket	Crítico	Criação de um Ticket Kerberos falso usando o hash da conta KRBTGT, permitindo acesso total ao domínio.	Proteger o hash KRBTGT; resetar a conta KRBTGT periodicamente; implementar MFA; monitorar DCs.
DCShadow	Crítico	Criação de um DC malicioso que injeta objetos e alterações diretamente no AD, burlando os logs tradicionais.	Restringir acesso administrativo; monitorar alterações no AD.
DCSync	Crítico	Abuso de permissões de replicação do AD para solicitar dados de senha de qualquer usuário, incluindo admins.	Restringir permissões de replicação (DS-Replication-Get-Changes); monitorar eventos ID 4662 e 4742.
Pass-the-Hash (PtH)	Alto	Uso de hashes NTLM em vez de senhas para autenticar em serviços, sem necessidade de conhecer a senha.	Implementar LAPS; desabilitar NTLM; segmentar privilégios; aplicar Tiered Administration.
Pass-the-Ticket (PtT)	Alto	Uso de tickets Kerberos (TGT) roubados para autenticação em serviços, sem credenciais em texto claro.	Habilitar proteção de Kerberos (KRB-SIGN, KRB-ENC); rotacionar tickets e senhas periodicamente.

Silver Ticket	Alto	Geração de tickets de serviço falsificados usando o hash do serviço, sem necessidade de comunicação com DC.	Proteger contas de serviço; restringir SPNs; usar Kerberos com assinatura e criptografia.
Kerberoasting	Alto	Solicitação de tickets de serviço (TGS) para contas configuradas com SPNs e tentativa de quebra offline da senha.	Usar senhas fortes para contas de serviço; aplicar menor privilégio; monitorar requisições TGS.
Credential Dumping	Alto	Extração de credenciais diretamente da memória (LSASS) ou arquivos do sistema.	Habilitar LSASS Protection (RunAsPPL); usar Credential Guard; limitar acesso a máquinas sensíveis.
Relay Attacks (NTLM Relay)	Alto	Interceptação e redirecionamento de autenticações NTLM para serviços legítimos, assumindo identidade do alvo.	Desabilitar NTLM; implementar SMB Signing; aplicar EPA (Extended Protection for Authentication).
Overpass-the-Hash (Pass-the-Key)	Alto	Gera um TGT Kerberos usando o hash NTLM de uma conta, evitando o uso de senha em texto claro.	Proteger Kerberos; restringir acesso ao LSASS; reforçar autenticação com MFA.
Privilege Escalation (via ACLs e objetos mal configurados)	Alto	Abuso de permissões delegadas incorretamente em objetos do AD (ACLs, DACLs) para escalar privilégios.	Revisar e corrigir permissões; utilizar ferramentas como BloodHound e PingCastle para análise contínua.

Fonte: Autoria própria

5.2 MELHORIAS E AJUSTES DE VULNERABILIDADES

Com os resultados obtidos da ferramenta pingle castle em um ambiente configurado, pode-se tomar medidas de ajustes conforme elencadas na tabela abaixo:

Tabela 2: Medidas de ajustes

Atividade	Descrição / Medidas de Ajustes
Configuração de Cota de Máquinas	Necessidade de ajustar a cota de máquinas para zero no Active Directory visando prevenir a adição não autorizada de máquinas ao domínio.
Criação de Credenciais Específicas / Delegação de permissões	A criação de credenciais específicas para a adição de servidores ao domínio, com o objetivo de limitar o uso de credenciais de alto privilégio e aumentar a segurança, evitando delegações desnecessárias.
Gestão de contas	A importância de gerenciar contas sensíveis e privilegiadas destacando a necessidade de uma gestão rigorosa para evitar riscos de segurança, bem como o uso de contas de serviço com delegações específicas e a importância de configurar corretamente as permissões.
Revisão de Contas	Necessidade de revisar contas com atributos inseguros, que apresentava configurações de SPN e suporte a criptografia RC4 em contas de usuários.

Uso da Conta Administrator Built-in	A utilização da conta built-in levanta questões de segurança e rastreabilidade, uma vez que não é possível identificar facilmente quem realizou determinadas ações usando essa conta.
Delegações Desconhecidas	Remoção de delegações desconhecidas é uma ação necessária para manter a integridade e segurança da estrutura do AD.
Contas Administrativas Inativas	As contas inativas devem ser cuidadosamente analisadas e removidas se necessário.
Revisão de Permissões e Grupos Privilegiados	Efetuar a revisão de permissões e grupos privilegiados, especialmente em relação à marcação de contas como sensíveis e delegadas, para evitar uso indevido.
Configuração de Contas de Serviço	É importante configurar contas de serviço com privilégios adequados para leitura e gerenciamento, visando otimizar o funcionamento.
Detecção e Resposta Automática	Importante configurar corretamente as ferramentas de segurança para garantir que elas funcionem de forma correta e protejam os recursos da organização.
Revisão de Políticas de Segurança	Revisar e ajustar as políticas de segurança, especialmente em relação à auditoria avançada.
Contas Privilegiadas	As contas com privilégios elevados devem ser monitoradas continuamente, pois sua exposição pode ser um vetor para ataques.
Revisão de Contas e Senhas	Necessidade da revisão de contas com configurações inseguras para fortalecer a segurança da rede.

Fonte: Autoria própria

6. CONCLUSÃO

A segurança do Active Directory representa um pilar essencial para a proteção da infraestrutura de TI nas organizações modernas, uma vez que esse serviço centraliza a autenticação, autorização e o gerenciamento de identidades (Conrad & Misenar, 2022). Este artigo demonstrou que, embora o AD ofereça uma estrutura robusta, ele também é um vetor crítico de ataque, especialmente diante de configurações inadequadas, privilégios excessivos e falta de monitoramento contínuo (CERT-BR, 2024; CrowdStrike, 2024). A adoção de boas práticas recomendadas com implementação de soluções como hardening, segmentação de rede, monitoramento de eventos e autenticação multifator é fundamental para mitigar riscos (Schroeder & Barnum, 2022). Em suma, proteger o Active Directory vai além da configuração técnica: exige uma abordagem estratégica e contínua de gestão de riscos, treinamento de pessoal e atualização frente às ameaças emergentes no cenário cibernético que devem ser mantidas periodicamente em sua organização (Martínez-Blasco et al., 2023).

Melhoria Contínua e Monitoramento

Além de identificar problemas pontuais, o uso periódico dessa ferramenta chamada pingle castle possibilitou a implementação de um ciclo contínuo de monitoramento, garantindo a rápida detecção e correção de novas vulnerabilidades à medida que surgem (Ferreira & Mattos, 2022). Este processo é essencial para manter a integridade do ambiente corporativo frente o avanço constante das ameaças cibernéticas (Grimes, 2022).

7. REFERÊNCIAS BIBLIOGRÁFICAS

1. ALEROUD, A.; ZHOU, L. *Cybersecurity risk assessment for Active Directory: Modeling privilege escalation and lateral movement*. Journal of Information Security and Applications, v. 70, p. 103517, 2023.

2. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO 31000:2018 – Gestão de riscos – Diretrizes. Rio de Janeiro: ABNT, 2018.

3. CENTER FOR INTERNET SECURITY (CIS). *CIS Controls v8: Controls, Safeguards & Implementation Group (IG) Assignment*. 2021. Disponível em: https://www.cisecurity.org/controls/cis-controls-list. Acesso em: 29 maio 2025.

4. CERT BR – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. *Alerta 05/2024 – Ameaças avançadas a ambientes Active Directory*. Brasília: NIC.br, 2024. Disponível em: https://cert.br. Acesso em: 29 maio 2025

5. CONRAD, Eric; MISENAR, Seth. *Microsoft 365 Certified: Identity and Services – Exam Guide*. 2. ed. Birmingham: Packt Publishing, 2022.

6. COSTA, D.; FERREIRA, M. *Análise de ataques cibernéticos direcionados ao Active Directory e estratégias de mitigação*. Journal of Information Security, v. 12, n. 3, p. 120-134, 2023.

7. CROWDSTRIKE. *2024 Global Threat Report*. Sunnyvale, CA: CrowdStrike, 2024.

8. FERREIRA, R.; MATTOS, P. *Gestão de vulnerabilidades no Active Directory: Uma abordagem baseada em análise contínua*. Revista Brasileira de Segurança da Informação, v. 14, n. 1, p. 45-62, 2022.

9. HOHMAN, Rob. *Cyber Defense Techniques for Active Directory Security*. 1. ed. New York: Apress, 2023.

10. INSTITUTO NACIONAL DE PADRÕES E TECNOLOGIA (NIST). *Security and Privacy Controls for Information Systems and Organizations (SP 800-53 Rev. 5)*. 2020. Disponível em: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final. Acesso em: 15 fev. 2024.

11. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. Genebra: ISO, 2022.

12. JONES, B.; JOHNSON, R. *Active Directory Security: Best Practices and Attack Mitigation*. 2. ed. New York: Apress, 2021.

13. KIRKLAND, Sean; MARTIN, Jason. *Securing Active Directory: How to Defend Against Modern Cyber Threats*. 1. ed. O'Reilly Media, 2021.

14. LAPS. *Local Administrator Password Solution (LAPS)*. Microsoft, 2024. Disponível em: https://www.microsoft.com/en-us/download/details.aspx?id=46899. Acesso em: 08 ago. 2024.

15. MARTÍNEZ BLASCO, Álvaro; GÓMEZ VILLEGAS, María; PÉREZ ARROYO, Diego. *Active Directory hardening strategies in hybrid infrastructures*. Journal of Cyber Security Technology, v. 7, n. 2, p. 147–168, 2023.

16. MELO, R.; SOUZA, T. *Mitigação de vulnerabilidades no Active Directory: Uma abordagem baseada em auditoria e conformidade*. Revista Brasileira de Segurança da Informação, v. 8, n. 2, p. 45-60, 2023.

17. METCALF, Sean. *Active Directory Security: Defending against modern threats*. Washington, DC: Trimarc Research, 2021.

18. METCALF, Sean; NELSON, Michael. *Attacking and Defending Active Directory: The Complete Guide*. 2. ed. Trimarc Press, 2022.

19. MICROSOFT. *Limite padrão para o número de estações de trabalho que um usuário pode ingressar no domínio*. Artigo. Publicado em 15 jan. 2025. Disponível em: https://learn.microsoft.com/pt-br/troubleshoot/windows-server/active-directory/default-workstation-numbers-join-domain. Acesso em: 15 jun. 2025.

20. MICROSOFT. Security Domains Controllers Against. 2024. Disponível em: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/securing-domain-controllers-against-attack. Acesso em: 07 nov. 2024.

21. MICROSOFT. *Security Considerations for Active Directory*. Microsoft Learn, 2023. Disponível em: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory. Acesso em: 29 maio 2025.

22. MICROSOFT. *Windows Defender Advanced Threat Protection for Identity Security*. 2023. Disponível em: https://learn.microsoft.com/pt-br/defender-for-identity/what-is. Acesso em: 05 mai. 2024.

23. MICROSOFT. *Active Directory Domain Services overview*. Publicado em 11 mar. 2025. Disponível em: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview. Acesso em: 14 jun. 2025.

24. NEMETH, C. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. 1. ed. New York: Oxford University Press, 2023.

25. PFEIFFER, Sylvain. *PingCastle Documentation: Active Directory Security Assessment Tool*. 2023.

26. PING CASTLE. *Ping Castle Documentation*. 2023. Disponível em: https://www.pingcastle.com/. Acesso em: 04 abr. 2025.

27. SANDERS, C. *Practical Windows Security*. 1. ed. Sebastopol: O'Reilly Media, 2022.

28. SCHROEDER, Will; BARNUM, Matt; SCOTT, Andy. *The Active Directory Attack and Defense Playbook.* SpecterOps, 2022. Disponível em: https://specterops.io/assets/resources/ActiveDirectory_Attack_and_Defense.pdf. Acesso em: 29 maio 2025.

29. TARANTINO, Anthony. *Governança corporativa de TI: usando as melhores práticas para manter a segurança e a conformidade*. Tradução: Jorge Ritter. Rio de Janeiro: Elsevier, 2008.