Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

Curso Superior de Tecnologia em Segurança da Informação

Dality Cristina Tamarozzi

Vitor Henrique de Rissio

TÉCNICAS DE DETECÇÃO E PREVENÇÃO DE ATAQUES DE DIA ZERO

Americana, SP

2025

FACULDADE DE TECNOLOGIA DE AMERICANA "Ministro Ralph Biasi"

Curso Superior de Tecnologia em Segurança da Informação

Dality Cristina Tamarozzi

Vitor Henrique de Rissio

TÉCNICAS DE DETECÇÃO E PREVENÇÃO DE ATAQUES DE DIA ZERO

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação na área de concentração sob a orientação do Prof.(a) Me. Clerivaldo Jose Roccia

Área de concentração: Segurança da Informação.

Americana, SP

2025

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana Ministro Ralph Biasi- CEETEPS Dados Internacionais de Catalogação-na-fonte

RISSIO, Vítor Henrique

Técnicas de detecção e prevenção de ataques de dia zero. / Vítor Henrique Rissio, Dality Cristina Tamarozzi – Americana, 2025.

106f.

Monografia (Curso Superior de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana Ministro Ralph Biasi – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Ms. Clerivaldo Jose Roccia

1. Segurança em sistemas de informação 2. Sistemas operacionais 3. Telemetria. I. RISSIO, Vítor Henrique, II. TAMAROZZI, Dality Cristina III. ROCCIA, Clerivaldo Jose IV. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana Ministro Ralph Biasi

CDU: 681.518.5
681.3.066
681.6

Elaborada pelo autor por meio de sistema automático gerador de ficha catalográfica da Fatec de Americana Ministro Ralph Biasi.

Dality Cristina Tamarozzi

Vitor Henrique de Rissio

Técnicas de detecção e prevenção de ataques de dia zero

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Curso Superior de Tecnologia em Segurança da Informação pelo Centro Paula Souza – FATEC Faculdade de Tecnologia de Americana Ministro Ralph Biasi.
Área de concentração: Segurança da informação.

Americana, 01 de dezembro de 2025.

Banca Examinadora:

Clerivaldo José Roccia
Mestre
Fatec Americana "Ministro Ralph Biasi"

José William Pinto Gomes
Especialista
Fatec Americana "Ministro Ralph Biasi"

Ivan Menerval da Silva
Doutor
Fatec Americana "Ministro Ralph Biasi"

AGRADECIMENTOS

Em primeiro lugar agradecemos ao professor Clerivaldo pelo apoio e orientação durante a estruturação deste trabalho. Também prestamos agradecimento a nós mesmos, pela dedicação e esforço ao seguir em frente diante dos desafios e obstáculos que surgiram. Por fim, agradecemos a instituição por dispor de recursos que utilizamos para desenvolver nosso trabalho.

RESUMO

Este trabalho apresentou uma visão teórica abrangente sobre os principais conceitos relacionados à segurança da informação e às ameaças digitais, incluindo os ataques de dia zero, que se caracterizam por explorarem vulnerabilidades ainda desconhecidas pelos fabricantes. Também foram discutidos aspectos jurídicos pertinentes, envolvendo responsabilidades e implicações legais relacionadas a incidentes cibernéticos. Para contextualizar o tema, apresentou-se um exemplo real de exploração, destacando as principais informações acerca do caso. Diferentes técnicas de detecção e prevenção foram abordadas teoricamente ao longo do trabalho e duas delas foram escolhidas e aplicadas na prática em um ambiente controlado, permitindo avaliar sua eficácia prática diante de um cenário simulado de teste. Os resultados obtidos foram positivos e evidenciaram que as abordagens selecionadas contribuem significativamente para a identificação redução dos riscos associados aos ataques de dia zero. O estudo destaca, por fim, a importância de combinar métodos de defesa, integrando soluções tecnológicas, como forma de fortalecer a proteção dos sistemas frente ao crescimento constante e à complexidade das ameaças cibernéticas.

Palavras-Chave: ataques de dia zero; segurança da informação; detecção; prevenção

ABSTRACT

This work presented a comprehensive theoretical overview of the main concepts related to information security and digital threats, including zero-day attacks, which are characterized by the exploitation of vulnerabilities still unknown to manufacturers. Relevant legal aspects were also discussed, involving responsibilities and legal implications associated with cybersecurity incidents. To contextualize the topic, a real exploitation case was presented, highlighting the key information related to the event. Different detection and prevention techniques were theoretically addressed throughout the study, and two of them were selected and practically applied in a controlled environment, allowing the assessment of their effectiveness in a simulated testing scenario. The results were positive and demonstrated that the selected approaches contribute significantly to identifying and reducing the risks associated with zero-day attacks. Finally, the study emphasizes the importance of combining defense methods and integrating technological solutions as a means to strengthen system protection in the face of the continuous growth and increasing complexity of cyber threats.

Keywords: *information security, zero-day attacks, detection, prevention.*

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

TI	Tecnologia da Informação
LGPD	Lei Geral de Proteção de Dados
GDPR	Regulamento Geral sobre a Proteção de Dados
USD	Dólar Americano
OWASP	Projeto aberto de Segurança de aplicações Web
CVE	Vulnerabilidades e Exposições Comuns
CWE	Enumeração de Fraqueza Comum
CVSS	Sistema Comum de Pontuação de Vulnerabilidades
FIRST	Fórum Global de Resposta a Incidentes e Equipes de Segurança
ISO	Organização Internacional de Padronização
RFC	Solicitação de Comentários
NIST	Instituto Nacional de Padrões e Tecnologia
ANPD	Agência Nacional de Proteção de Dados
GTIG	Google Threat Intelligence Group
SMBv1	Server Message Block versão 1
CVE	Vulnerabilidades e Exposições Comuns
EDR	Detecção e Resposta de Endpoint
API	Interface de Programação de Aplicativos
WDEG	Windows Defender Exploit Guard
ASR	Redução da Superfície de Ataque
OSVDB	Open-Source Vulnerability Database
URL	Uniform Resource Locator
MD5	Message-Digest Algorithm 5
SHA256	Secure Hash Algorithm 256-bit

EICAR	Instituto Europeu de Pesquisa em Antivírus de Computador
CARO	Organização de Pesquisa de Antivírus de Computador
ASCII	Código Padrão Americano para Intercâmbio de Informação
HTTP	Hypertext Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
FTP	File Transfer Protocol
VM	Máquina Virtual
NAT	Tradução de Endereços de Rede
DHCP	Protocolo de Configuração Dinâmica de Host
JSON	Notação de Objetos JavaScript
SSH	Shell Seguro
GUID	Identificador Globalmente Único
SIEM	Gerenciamento de Informações e Eventos de Segurança
IOC	Indicadores de comprometimento
IOA	Indicadores de ataque

SUMÁRIO

INTRODUÇÃO

No contexto contemporâneo, o ativo informação assume papel fundamental para organizações e indivíduos, sendo alvo constante de ameaças cibernéticas que buscam comprometer sua confidencialidade, integridade e disponibilidade. A crescente digitalização e interdependência entre sistemas intensificaram a exposição a vulnerabilidades, destacando-se os ataques de dia zero, caracterizados pela exploração de falhas desconhecidas até então, sem correções disponíveis. Conforme Oliveira e Waldman (2021), a compreensão do conceito de informação é essencial para fundamentar a defesa cibernética, vista como um campo da ciência da computação que visa proteger esses ativos valiosos. A segurança da informação, por sua vez, é definida como o conjunto de ações destinadas a proteger os dados contra acessos não autorizados, perdas ou danos, conforme (Campos, 2007 apud Silva; Nascimento, 2022).

Diante da crescente ocorrência e da complexidade dos ataques de dia zero, que se tornaram um dos principais desafios da segurança da informação, este trabalho se debruçou no seguinte problema de pesquisa: como investigar e aplicar técnicas eficazes para a detecção e prevenção de ataques de dia zero, promovendo uma solução eficaz contra-ataques de dia zero no contexto da Segurança da Informação? Dessa forma, a importância desse trabalho reside na crescente ocorrência e complexidade dos ataques de dia zero, que se tornaram um dos principais desafios relacionados à segurança da informação. A falta de correções prévias para essas vulnerabilidades gera a necessidade do desenvolvimento de técnicas para detecção e prevenção desses ataques.

O objetivo geral deste trabalho foi abordar conceitualmente técnicas eficazes para a detecção e prevenção de ataques de dia zero, além de promover um laboratório prático aplicando uma técnica de cada tipo abordada anteriormente, concretizando assim, uma solução para o problema de pesquisa.

A metodologia utilizada caracteriza-se como exploratória qualitativa, fundamentada em revisão bibliográfica, artigos científicos, publicações especializadas, fonte técnicas e experimentação prática. Essa abordagem permitiu a coleta e análise detalhada de dados relativos aos métodos escolhidos em ambiente simulado composto por máquinas virtuais Linux e Windows. Conforme Gil (2008), a

pesquisa exploratória tem como finalidade desenvolver, esclarecer e modificar conceitos existentes, orientando novas investigações e validações de hipóteses, o que embasou a realização do laboratório prático aplicado as técnicas escolhidas juntamente com as análises dos resultados.

Este trabalho está organizado em cinco capítulos. O Capítulo 1 é a presente introdução. O Capítulo 2 o referencial teórico introduz os fundamentos teóricos, explicando desde o conceito de informação, a importância da segurança da informação e seus pilares, até a apresentação detalhada de três técnicas de detecção e três de prevenção de ataques de dia zero. O Capítulo 3 a metodologia descreve a seleção, explicação e aplicação de duas técnicas, uma de cada tipo, para detecção e prevenção de ataques de dia zero, detalhando a preparação do ambiente para a aplicação, juntamente com a explicação dos métodos. Os métodos escolhidos foram: detecção baseado em análise de dados e prevenção utilizando o Windows Defender Exploit Guard, que resultaram na apresentação do trabalho prático. O Capítulo 4 a análise de resultados apresenta a análise e os resultados obtido nos experimentos, evidenciando a eficácia do método de detecção e prevenção do ambiente simulado. O Capítulo 5 se reserva às considerações finais, com base nas informações conseguidas a partir dos estudos realizados.

1 REFERENCIAL TEÓRICO

1.1 Conceito de Informação

Uma das características do período contemporâneo é a sistemática perda de significado etimológico das palavras, nas quais sofrem alteração no seu significado para se adequar a cada discurso diferente, este problema decorrente de uma inexatidão conceitual ou próprio desconhecimento, aflige diversas áreas do conhecimento científico incluindo a computação, área na qual se tem a palavra informação como alvo dessa descaracterização etimológica (Oliveira; Waldman, 2021).

A ciência da computação é definida por Saracevic (1996 apud Oliveira e Waldman, 2021) como um campo de estudo que tem por objetivo o estudo e a análise de problemas informacionais. Ela utiliza o conceito de informação para diversas áreas de estudo incluindo a defesa cibernética, no entanto, para se ter uma compreensão plena teórica, necessita-se que tenha um conhecimento prévio conceitual no que diz respeito ao ativo de valor informação, entendendo sua importância e impacto social e individual aos responsáveis. Portanto, essa seção visa conceituar informação através da ótica da Ciência da Informação, posteriormente fornecendo bagagem para abordar a crescente importância na sociedade contemporânea e demais tópicos.

Segundo Buckland (1991 *apud* Oliveira e Waldman, 2021), em seu artigo que analisa o conceito de informação, são estabelecidos três principais significados para o termo informação: processo, conhecimento e coisa. Esses significados são analisados sob duas principais perspectivas: tangibilidade ou intangibilidade, e entidade ou processo. Para o autor, a informação como processo corresponde àquele que gera transformação no conhecimento, ou seja, ao recebimento de um novo conteúdo, trata-se de um processo intangível, independente de suporte físico. Já a informação como conhecimento é o objeto do processo informacional, que precisa ser explicado por meio de processos comunicacionais para ser compreendido, configurando-se, portanto, como uma entidade intangível. Por fim, a informação como coisa refere-se a um objeto manipulável no mundo físico, como um documento que contém conhecimento, caracterizando-se como uma entidade tangível.

Elucidando esse pensamento, informação como processo seria um analista ou um profissional de segurança aprendendo sobre uma nova técnica de engenharia social. Durante o treinamento, ele aprende como e-mails podem ser personalizados para enganar os usuários, esse aprendizado é um processo informacional, pois a informação recebida transforma o conhecimento do analista, permitindo que ele identifique e previna esse tipo de ataque no futuro, a informação como processo está vinculada à compreensão e assimilação do conteúdo que transformou o analista.

Informação como conhecimento é o objeto do processo informacional, um analista que descobre uma vulnerabilidade em um software, por intermédio de testes, precisa comunicar essa informação com sua equipe, através, por exemplo, de um relatório técnico. A informação como conhecimento, neste caso, é a própria compreensão da vulnerabilidade, que só se torna útil quando expressa e compartilhada por meio de linguagem, diagramas ou outros canais de comunicação.

Por fim, a informação como coisa refere-se, por exemplo, a um documento detalhando a vulnerabilidade encontrada em um software, incluindo descrição técnica, recomendações para mitigações etc. O relatório é a informação como coisa, pois é um meio físico, manipulável e tangível, que fornece o conhecimento da vulnerabilidade.

Segundo Buckland (1991), alguns teóricos têm rejeitado o uso do termo informação como coisa, Wiener, citado por Buckland (1991, p.352), assegura que “informação é informação, não um material e nem energia”. Já Machlup e Faithorne, também citados por Buckland (1991), restringem informação ao contexto da comunicação, definindo-a como um atributo do conhecimento recebido e da interpretação do sinal, não do remetente.

Buckland (1991) prossegue dizendo que a linguagem possui suas limitações e que o termo informação como coisa não deve ser dispensado até que seja compreendido como o significado real de informação, pois em sistemas de informação, a informação não pode existir como conhecimento fundamentado ou processo de acesso ao conhecimento, mas sim como representações físicas do conhecimento que possam ser manipuladas, operacionalizadas, armazenadas e recuperadas.

Outras definições de informação também foram apresentadas, Mattelart conforme citado por Oliveira e Waldman (2021), recorre a um sentido matemático abordando a Teoria Matemática da Comunicação, de Claude Elwood Shannon,

afirmando que “a definição de informação é estritamente física, quantitativa, estatística. Trata-se sobretudo de quantidade de informação” (Mattelart, 2006 *apud* Oliveira; Waldman, 2021, p. 250).

Por sua vez, Amaral (2008 apud Oliveira; Waldman, 2021, p. 250), em um estudo com foco econômico, aborda a informação como uma “mensagem, geralmente sob a forma de um documento ou em uma comunicação audível e/ou visível, numa versão enriquecida de dados, uma vez que inclui algo sobre o contexto que permita retirar algum significado”.

Já Castells (2016 *apud* Oliveira; Waldman, 2021, p. 250), através de uma abordagem sociológica, o autor entende a informação como produto da sociedade dizendo que: “a emergência de um novo paradigma tecnológico, organizado em torno de novas tecnologias da informação, mais flexíveis e poderosas, possibilita que a própria informação se torne o produto do processo produtivo”.

Portanto, para conceituar de forma generalizada, este trabalho adotará as definições colocadas pelos pesquisadores Oliveira e Waldman (2021, p. 251-252).

> A informação é recurso e produto final no processo produtivo, considerando-se que é utilizada para a produção de mais informação, tanto quanto é o resultado dessa produção. Possui valor mercadológico, financeiro, de forma independente, decorrente de sua capacidade de atribuir valor a produtos e serviços, o que pode ser aferido de formas diversas a depender do seu tempo de difusão. E possui um valor potencial, decorrente de seu uso futuro, ainda incerto na forma, mas certo no poder.

1.2 Importância da Informação na Sociedade Contemporânea

Na sociedade global atual, a realidade já não se restringe a um conjunto de nações que coexistem separadamente, tampouco tem como foco exclusivo o indivíduo ou a coletividade local, mas passa a ser moldada pela constituição de uma sociedade global estruturada por uma interdependência e fundamentada pela globalização (Andrada, 2001). Essas transformações evidenciam que as relações globais se desenvolveram de forma a constituir uma interconexão em nível global, de modo que a conectividade resultante se tornou uma dependência necessária para a sociedade contemporânea. Nessa nova forma de organização social, causada pela estabilização da tecnologia, evidencia-se um diferencial importante em relação às mudanças tecnológicas do passado: o domínio da informação e do conhecimento (Andrada, 2001). A aplicação dessa mudança no contexto histórico resultou, de acordo com Bell

(1973 *apud* Webster, 1993), em uma sociedade pós-industrial, marcada pela relevância crescente da informação em todos os aspectos sociais.

Abrams (2021 *apud* Carvalho, 2025) afirma que existem 4,7 bilhões de usuários ativos nas redes sociais, número que representa 59% da população mundial, o que equivale a mais da metade dos habitantes do planeta que acessam as redes sociais de forma contínua. Esses números mostram a relevância da informação em todos os aspectos sociais e a dependência necessária em relação a ela, que se originou da conectividade em toda a sociedade contemporânea.

Um exemplo disso é o surgimento de diversos influenciadores, profissão que utiliza as redes sociais como ferramentas de trabalho e, a partir disso, obtém ganhos monetários, tornando-a muito almejada (Carvalho, 2024 *apud* Carvalho, 2025). Dessa forma, a sociedade contemporânea é marcada pela relevância da informação, transformando as relações sociais e, consequentemente, tornando-a o principal ativo de valor global.

Segundo a definição de Webster (1993), a informação pode ser conceituada como inteligência ou instrução sobre algo ou alguém. A importância dela no período atual se dá, segundo Werthein (2000), pela mudança do fator-chave, que antes era definido pela energia, mas que agora é caracterizado por insumos baratos de informação, como resultado dos avanços na microeletrônica e nas telecomunicações.

A informação, nessa nova forma de uso da tecnologia, tornou-se imprescindível tanto no contexto das organizações quanto em todos os outros aspectos sociais. Dessa forma, ela influencia diretamente a participação política, social, econômica e comercial da sociedade (Camargo, 2017). Assim, cada setor social utiliza, propaga e a modifica como parte central de sua atividade, alocando também nesse escopo as organizações, que, por sua vez, têm-na como fator central de sua vantagem competitiva.

De acordo com Moresi (2000), a adequação a essa mudança permite um diferencial de mercado aliado a uma lucratividade. A informação, dessa forma, se torna um recurso-chave para as empresas, e sua gestão adequada determina o sucesso organizacional, tornando-a um fator estruturante e um instrumento de gestão. Portanto, o termo sociedade da Informação se consolida na forma de período em que a economia passou a ser baseada na informação, na tecnologia e nas telecomunicações (Delbianco; Valentim, 2025).

1.3 Sociedade da informação

De acordo com Ferreira (2002), a sociedade da informação se define pela aplicação geral da tecnologia em todos os setores da sociedade, na forma de processamento, armazenamento e transmissão dos dados, os quais transformaram a sociedade pós-industrial.

Destaca-se que o período que contempla a Segunda Guerra Mundial e a Guerra Fria trouxe transformações relevantes no que se refere aos avanços nos meios de comunicação e na disseminação de conhecimento, inclusive de cunho científico, decorrentes do desenvolvimento das tecnologias de comunicação (Delbianco; Valentim, 2025). Essas alterações são marcantes no século XXI justamente pelas transformações sociais significativas que surgiram com o avanço da tecnologia (Kohn; Moraes, 2007).

Nesse contexto, o termo sociedade da informação começou a ser utilizado para destacar exatamente estas mudanças originárias dos avanços tecnológicos, organizacionais e administrativas (Werthein, 2000). Um dos fatores desse avanço da tecnologia foi o surgimento de mecanismos computacionais para que as informações pudessem ser difundidas, processadas e armazenadas, de modo a serem utilizadas de forma inteligente e efetiva na tomada de decisão, satisfazendo os diferentes níveis operacionais e gerenciais (Santos, 2009).

Como consequência disso, esses sistemas se tornaram alvo de interesse principal para os criminosos, uma vez que os dados habitam ambientes intangíveis e abstratos, tornam-se constantemente vulneráveis às ameaças, principalmente em organizações que não implementam medidas eficazes de proteção, gerando um alto risco para a segurança da informação (Coutinho *et al*., 2017).

1.4 Sistemas de Informação

O processamento dos dados envolve a operação sincronizada de diversos componentes, os quais recebem o nome de sistemas de informação. A definição de sistemas de informação é descrita, segundo Stair e Reynolds (2009), como um conjunto de componentes inter-relacionados que coletam, processam, armazenam e distribuem informações, que são usadas para apoiar a tomada de decisões, a coordenação, o controle, a análise e a visualização nas organizações.

Assim, um sistema de informação em uma organização é entendido como o conjunto de registros e documentos gerados nas operações organizacionais, podendo ser manuais ou informatizados (Cassarro, 2010 *apud* Jannuzzi; Falsarella; Sugahara, 2014). Juntamente com isso, os sistemas de informação integram-se entre si, pois não se limitam ao *hardware* e ao *software*, mas também envolvem o alinhamento da TI com a estratégia organizacional (Laurindo *et al*., 2001).

Para Laudon e Laudon (2010 *apud* Jannuzzi; Falsarella; Sugahara, 2014), as organizações estão direcionando esforços para sistemas que integram as atividades das unidades e dos processos dos negócios, os processos organizacionais definidos como um conjunto de atividades integradas que estabelecem como tarefas organizacionais específicas serão realizadas.

Portanto, a organização funciona em um ambiente amplo de informações que realiza a coleta, armazenamento e manipulação dos dados (Stair; Reynolds, 2008). Essa estrutura depende dos recursos organizacionais e dos sistemas de informação, que se tornaram alvo de criminosos digitais devido à sua crescente importância, o que exige atenção tanto no espaço físico quanto no ambiente virtual das instituições.

1.5 Segurança da Informação

Consequentemente, os sistemas de informação tornaram-se alvos dos criminosos digitais, ameaçando o comprometimento de toda uma estrutura organizacional. Esse contexto destaca a importância do estudo da segurança da informação, que se apresenta como a única forma de proteger os ativos das organizações. A definição de segurança da informação, segundo Campos (2007 *apud* Silva; Nascimento, 2022, p. 5), é descrita como:

> A definição para a segurança da informação está diretamente ligada em proteger dados de propriedade das organizações e ou sob sua guarda, podendo ser de pessoa física e jurídica, nas quais requerem esforços para garantir a mitigação de riscos e a continuidade das operações.

Segundo Holdsworth e Kosinski (2024), os termos segurança da informação, segurança de TI, cibersegurança e segurança de dados são frequentemente e incorretamente utilizados como sinônimos, porém diferem, principalmente, no escopo de cada um deles:

Segurança da informação é um termo abrangente, que envolve os esforços de uma organização para proteger as informações desde a segurança física e a segurança dos dispositivos finais até a criptografia e a segurança de redes, entre outros aspectos.

Segurança de TI inclui também a proteção dos ativos físicos e digitais de TI e dos *data centers*, mas não envolve a proteção para armazenamento de arquivos em papel e outras mídias, concentra-se nas ferramentas tecnológicas, e não nas informações em si.

Segurança cibernética concentra-se na proteção dos sistemas de informação digitais, seu escopo é proteger os dados e ativos digitais contra ameaças cibernéticas, a segurança cibernética não se preocupa em proteger dados analógicos ou em papel.

Segurança de dados é a prática de proteger informações digitais contra acesso não autorizado, corrupção ou roubo de dados incluindo a segurança física dos dispositivos de *hardware* e armazenamento, além de controles administrativos e de acesso, inclui-se também a segurança lógica dos *softwares* e as políticas da organização.

Holdsworth e Kosinski (2024) também destacam que uma violação de informações confidenciais de uma empresa ocasiona perda de clientes e danos consideráveis, provavelmente irreparáveis, à sua reputação, além de prejudicar sua rentabilidade e minar sua vantagem competitiva. Concomitantemente, a violação de dados também implica enfrentar multas regulatórias e penalidades legais, a Lei Geral de Proteção de Dados (LGPD) e o Regulamento Geral de Proteção de Dados (GDPR) são exemplos, respectivamente, nacional e europeu, de marcos regulatórios que exigem que as empresas protejam as informações confidenciais dos clientes.

Ademais, ainda citando Holdsworth e Kosinski (2024), o Relatório de Custo de uma Violação de Dados da empresa IBM, revela que o custo total médio de uma violação de dados atingiu um marco de USD 4,45 milhões em 2023, representando um aumento de 15,3% em relação aos USD 3,86 milhões do relatório de 2020.

No Brasil, as pequenas e médias empresas representam em torno de 30% do Produto Interno Bruto, e muitas delas utilizam a tecnologia como parte essencial do seu trabalho seja provendo serviços, seja organizando seus processos. No entanto, em relação à segurança digital, elas ainda são extremamente vulneráveis, o que permite que um ataque possa ser definitivo para o fim de suas atividades. De acordo com as pesquisas mais relevantes, mais de 50% de todos os ataques cibernéticos nos

anos recentes visam computadores e usuários das pequenas e médias empresas (Vale *et al*., 2022).

Soma-se a isso o que a TI INSIDE (2024) afirma: “O Brasil é o país mais vulnerável a ataques cibernéticos da América Latina. De acordo com a pesquisa publicada em 2023, no primeiro semestre foram 23 bilhões de ataques contra o Brasil, o que representa 36% do total na América Latina.” Ainda sobre segurança cibernética, a matéria aponta que: “43% dos brasileiros apontaram o tema como fator que ameaça o crescimento das companhias acima da média da América Latina de 35%, e menor que a média global, que ficou em 50%”.

Corroborando esse fato, outra matéria da TI INSIDE (2025) apresenta que: “O mercado brasileiro de segurança da informação movimentará cerca de R$ 104,6 bilhões entre 2025 e 2028, com uma taxa de crescimento acumulada de 43,8%” Destaca-se também o crescente mercado de trabalho: “Entre 2015 e 2024, o número de profissionais empregados em segurança da informação apresentou uma taxa média anual de crescimento de 16,1%. Em 2023, 1.849 pessoas se graduaram em cursos relacionados à área, um aumento de 15,3% em relação ao ano anterior”.

John McCumber desenvolveu o Cubo de McCumber como uma maneira de gerenciar riscos. Esse modelo fornece ao profissional de segurança um meio de avaliar graficamente o risco de um sistema, visualizar o cubo de diferentes ângulos oferece ao profissional uma forma de considerar o risco sob diferentes perspectivas (Price, 2008; Figura 1).

Os estados da informação, conforme abordado por Price (2008), representam as condições em que as informações podem ser encontradas dentro de um sistema de informação, esses estados são:

Processamento: Informações mantidas em memória volátil ou manipulada através de um processador, como em operações realizadas por algoritmos;

Armazenamento: Isto refere-se a armazenamento não volátil de informações, como discos rígidos ou mídias de *backup*;

Transmissão: Informações transitando através da rede, seja ela interna ou da Internet.

Figura 1 – Cubo de McCumber

Fonte: Adaptado de Price (2008).

diversos estados. Essas medidas podem ser classificadas em três categorias principais:

Pessoas são todos os indivíduos relacionados a um sistema, incluindo administradores e usuários, que devem ser treinados a fim de evitar de serem instrumentos de ataque;

Políticas e práticas, refere-se a políticas documentadas e processos usados para orientar pessoas que interagem com o sistema, como por exemplo, separação de tarefas e controles de acesso;

Tecnologia, compreende-se os hardware e software que operam em sistemas, como sistemas operacionais, aplicativos, dispositivos de rede e ferramentas de segurança.

Por fim, os objetivos intangíveis de segurança de um sistema concentram-se na tríade confidencialidade, integridade e disponibilidade, que serão abordados posteriormente na próxima seção.

Dessa forma, a segurança da informação assegura a proteção dos recursos informacionais que permitem à organização alcançar seus objetivos institucionais e de negócios. Trata-se, portanto, de um processo organizacional voltado a garantir que

a instituição atinja suas metas no que se refere à gestão e proteção das informações e dos recursos informacionais (Fontes, 2015).

1.6 Pilares da segurança da informação

A construção de ambientes digitais seguros, garantindo que as informações estejam protegidas, confiáveis e acessíveis conforme a necessidade do negócio, fundamenta-se, conforme definido pela ISO Organização Internacional de Normalização, em tradução livre, em três princípios: confidencialidade, integridade e disponibilidade (Symbioti, 2025, Figura 2).

O primeiro princípio diz respeito à confidencialidade, cujas ferramentas tecnológicas de segurança visam proteger as informações, de modo que apenas os agentes autorizados tenham acesso, limitando, assim, o acesso a informações confidenciais (Sêmola, 2014 *apud* Klettenberg, 2016).

O segundo princípio, referente à integridade da informação, tem como objetivo a manutenção das características originais da informação, protegendo-a contra modificações indevidas. Dessa forma, apenas agentes autorizados podem realizar alterações legítimas, enquanto os não autorizados estão impedidos de fazê-lo (Peixoto, 2006; Sêmola, 2014 *apud* Klettenberg, 2016).

O terceiro princípio refere-se à disponibilidade, da qual se define como a capacidade de a informação ser acessada por qualquer agente e a qualquer tempo. Em outras palavras trata-se de garantir que os dados possam ser consultados de forma contínua e imediata sempre que necessário (Peixoto, 2006; Sêmola, 2014 *apud* Klettenberg, 2016). Outros três princípios aparecem, muitas vezes, juntamente com a tríade acima citada, são eles: autenticidade, não repúdio e conformidade, conforme Bastos (2023).

A autenticidade é um princípio que determina que as informações precisam ser verdadeiras e provenientes de fontes confiáveis. Estabelece-se, assim, que seja possível rastrear e atestar a veracidade das informações, identificando os agentes autores;

O não repúdio, ou irretratabilidade, é um princípio que estabelece que os agentes usuários não possam negar a autoria das informações, como forma de assegurar sua autenticidade. Assim, nem o agente autor nem o receptor podem contestar qualquer transação de dados;

Figura 2 – Princípios da segurança da informação

Fonte: Maia (2013) *apud* Klettenberg (2016).

A conformidade é um princípio que garante que todos os processos obedeçam às leis e às normas regulamentares. Para isso, as empresas devem desenvolver protocolos de acordo com essas normas e, além disso, promover meios de fiscalização que assegurem o cumprimento dos protocolos.

1.7 Vulnerabilidades em Segurança da Informação

Entender as vulnerabilidades exige relacioná-las diretamente aos pilares fundamentais da segurança da informação, pois cada falha pode comprometer um ou mais desses aspectos essenciais.

Segundo Ghelani, Hua e Koduru (2022), vulnerabilidade é uma falha ou ponto fraco em um sistema, ou na forma como ele foi desenvolvido, que pode ser explorado por um invasor para executar códigos maliciosos, acessar informações sem permissão ou realizar outros tipos de ataque, trata-se de uma fraqueza existente no sistema que, quando explorada, pode comprometer toda a sua estrutura. Complementando essa definição, a OWASP (2025) define vulnerabilidade, no contexto de aplicações, como uma falha ou fraqueza decorrente de erro de design ou *bug* de implementação, que permite que o invasor cause danos às partes interessadas. Essas definições evidenciam que as vulnerabilidades são fraquezas que exploradas representam uma ameaça à confidencialidade, à integridade e à disponibilidade dos sistemas.

As causas de vulnerabilidades estão mais frequentemente relacionadas a fatores humanos e técnicos. Conforme descrito por Malerba (2010), três motivos básicos contribuem para o surgimento de vulnerabilidades: erros de implementação, falhas de *design* e erros de configuração ou de infraestrutura do sistema. Corroborando, Carmo *et al*. (2021) destacam que mecanismos de segurança inadequados e ações mal-intencionadas também amplificam essas fraquezas, entre as vulnerabilidades mais comuns, destacam-se injeções de falhas, quebras de autenticação, exposição de dados sensíveis, configurações de segurança inadequadas e falhas no controle de acesso, essas fraquezas podem causar impactos significativos, desde vazamentos de dados até a paralisação de sistemas.

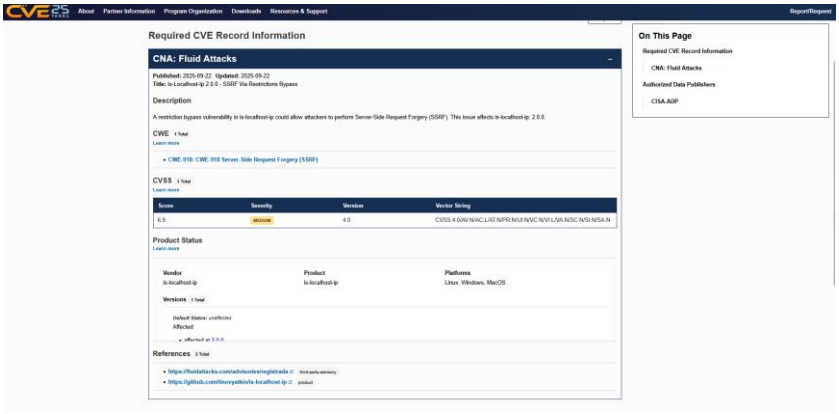
Para possibilitar o monitoramento e tratamento adequado dessas falhas, surgem mecanismos de catalogação e padronização, sendo os mais reconhecidos CVE (Vulnerabilidades e Exposições Comuns) e o CWE (Enumeração de Fraqueza Comum). Segundo a definição de Gueye *et al*. (2021), CVE é definido como:

> As Vulnerabilidades e Exposições Comuns (CVE) são um grande conjunto de vulnerabilidade divulgadas publicamente em softwares amplamente utilizados. Elas são enumeradas com um identificador único, descritas e referenciadas com avisos externos.

Para cada vulnerabilidade de segurança há um registro CVE que visa catalogar para consulta de organizações em todo mundo, profissionais de tecnologia da informação e segurança cibernética utilizam os registros de CVE para concentrar esforços e priorizar a abordagem em relação as vulnerabilidades (CVE, 2025).

O exemplo apresentado na Figura 3, refere-se à vulnerabilidade CVE-2025-9960, publicada em 22 de agosto de 2025. Essa falha consiste em um *by-pass* de restrições, que pode permitir a invasores executar comandos de falsificação no lado do servidor. Além disso, a vulnerabilidade é classificada com nível de severidade médio, o que evidencia o potencial de risco que representa. Assim, a identificação e monitoramento contínuo de vulnerabilidades tornam-se imprescindíveis para que as organizações mantenham seus sistemas protegidos diante das constantes mudanças tecnológicas.

Figura 3 – Exemplo de CVE



Fonte: CVE (2025).

Outra métrica utilizada na classificação de vulnerabilidades é a Enumeração de Fraqueza Comum (CWE), que oferece uma forma de categorizar e descrever tipos de vulnerabilidades de segurança em *softwares* e sistemas (CWE, 2023 *apud* Braz, 2023). A principal diferença entre CVE e CWE está no fato de o CVE identificar uma vulnerabilidade específica em um sistema, enquanto o CWE representa um conjunto de vulnerabilidades de segurança descritas em um nível mais abstrato (Souza, 2022 *apud* Braz, 2023).

Para Braz (2023), caso um tipo específico de falha seja identificado em diferentes produtos, isso se classificaria como CWE, já um caso particular dessa falha, em um produto específico, seria um CVE. Os projetos de CVEs, CWEs e o modelo ATT&CK são gerenciados pela organização sem fins lucrativos MITRE Corporation, dedicada ao avanço da ciência e da tecnologia (Mitre, 2023 *apud* Braz, 2023).

Outro fator importante é o gerenciamento de vulnerabilidades, que consiste na prática cíclica de identificar, classificar, remediar e mitigar vulnerabilidades, o mapeamento de vulnerabilidades identifica e analisa possíveis fraquezas dos sistemas (Moreno, 2017 *apud* Carmo *et al*., 2021). Dessa forma, o gerenciamento envolve identificar e classificar de forma prática e evidente uma ameaça para, posteriormente, remediar e mitigar as vulnerabilidades detectadas, fornecendo uma visão geral sobre grau de importância, impacto e meios de mitigação.

Um exemplo de gerenciamento e classificação de vulnerabilidades é o Sistema Comum de Pontuação de Vulnerabilidades (CVSS), que oferece uma maneira de avaliar as principais características de uma vulnerabilidade e produzir uma pontuação numérica que reflete sua gravidade. A pontuação é posteriormente representada de

forma qualitativa, sendo classificada como baixa, média, alta ou crítica. Dessa forma, o CVSS auxilia as organizações avaliarem e priorizarem adequadamente o processo de gerenciamento de vulnerabilidades (FIRST, 2025b).

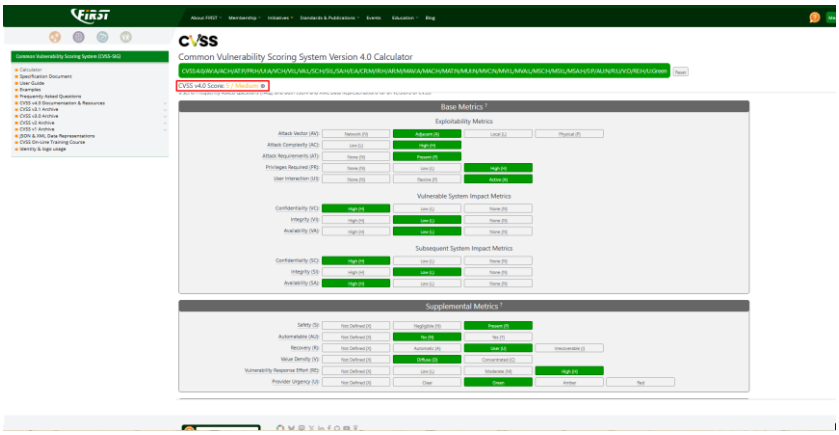
A pontuação básica do CVSS leva em consideração dois fatores principais: a explorabilidade, definida como a facilidade com que uma vulnerabilidade pode ser utilizada em um ataque, e o impacto, que corresponde à quantidade de dano que essa vulnerabilidade pode causar em um componente afetado, independentemente de qualquer ambiente específico (Gueye *et al.,* 2021). A métrica de explorabilidade é composta pelos seguintes elementos: vetor de ataque, que descreve o meio pelo qual o ataque pode ser conduzido; complexidade do ataque, que indica as condições externas ao controle do invasor necessárias para que a exploração ocorra; privilégios necessários, que definem o nível de acesso que o atacante deve possuir antes de explorar a vulnerabilidade; e interação com o usuário, que determina se a exploração depende da participação de um usuário para ser executada.

A pontuação de impacto fundamenta-se na avaliação dos efeitos sobre a confidencialidade, integridade e disponibilidade do sistema afetado. Além disso, a métrica de escopo é utilizada para identificar se uma vulnerabilidade em determinado componente pode afetar outros recursos ou componentes fora de seu escopo de segurança (Gueye *et al*., 2021).

A Figura 4 apresenta a ferramenta oficial do Sistema Comum de Pontuação de Vulnerabilidades (CVSS), versão 4.0, disponibilizada pelo FIRST. Ela calcula a pontuação de uma vulnerabilidade com base em métricas de explorabilidade, impacto e escopo, permitindo classificá-la conforme sua gravidade. No teste, o resultado das métricas oferecidas resultou em uma classificação considerada média para a vulnerabilidade apresentada. Dessa forma, tanto a identificação quanto a gestão das vulnerabilidades presentes na infraestrutura de TI são partes fundamentais da segurança da informação.

A ausência dessas práticas permite que vulnerabilidades não identificadas ou ainda sem correção constituam a base dos chamados ataques de dia zero, nos quais invasores exploram falhas desconhecidas antes que existam medidas de mitigação disponíveis, comprometendo os pilares fundamentais da segurança da informação.

Figura 4– Exemplo de classificação utilizando o CVSS 4.0



Fonte: FIRST (2025a).

1.8 Como vulnerabilidades se tornam ameaças

Como colocado anteriormente, as vulnerabilidades representam pontos fracos que podem comprometer a segurança da informação, nesse contexto, o conceito de ameaça refere-se à exploração efetiva dessas vulnerabilidades. Segundo Stallings e Brown (2018), ameaças são quaisquer circunstâncias ou eventos com potencial para comprometer as operações organizacionais, incluindo reputação, imagem, funções e missão institucional. Os autores afirmam que, para cada tipo de vulnerabilidade presente em um sistema, existem ameaças capazes de explorá-la, representando um risco potencial à segurança dos ativos. Quando concretizadas por meio de um ataque bem-sucedido, resultam em violações de segurança. Por fim, Stallings e Brown (2018) destacam que o responsável pela execução do ataque é denominado atacante ou agente da ameaça.

Complementando essa definição, Peltier (2010) define ameaça como um evento indesejado que pode impactar os objetivos ou a missão de negócio de uma organização. Segundo o autor, uma ameaça ocorre quando os processos internos existentes foram implementados de maneira incorreta ou perderam sua eficiência, gerando uma fraqueza que, ao ser explorada, compromete a função esperada do processo e, consequentemente, a infraestrutura como um todo. Essa ocorrência é conhecida como exploração de vulnerabilidade.

Peltier (2010), também classifica as ameaças em três tipos gerais, chamadas fontes de ameaça, classificando-as com base na sua natureza:

Ameaças naturais que são ameaças associas a causas naturais como enchentes, terremotos, tornados, deslizamentos de terra;

Ameaças humanas que são ameaças ocasionadas por ações geradas ou facilitadas por pessoas como erros e omissões, fraudes, uso de *softwares* maliciosos e acessos não autorizados;

Ameaças ambientais que são ameaças relacionadas a fatores ambientais como quedas prolongadas de energia, poluição, vazamentos químicos ou de líquidos, que podem afetar diretamente a infraestrutura e o funcionamento dos sistemas.

Dessa forma, as ameaças representam a materialização das vulnerabilidades, podendo comprometer processos, ativos e a missão organizacional. As definições de Stallings e Brown (2018) e de Peltier (2010) evidenciam que uma ameaça ocorre quando há exploração de fraquezas existentes, caracterizando uma violação da segurança. A classificação proposta por Peltier em ameaças naturais, humanas e ambientais demonstra que os riscos abrangem não apenas fatores tecnológicos, mas também elementos relacionados a processos, pessoas e ambiente, reforçando a importância de uma categorização precisa para análises de segurança mais eficazes.

1.9 Definição de ataque

Complementando o conceito de ameaça, um ataque consiste na exploração de uma vulnerabilidade por meio de uma ameaça, comprometendo a segurança dos sistemas e podendo violar políticas, serviços ou ativos organizacionais (Ferreira, 2010 *apud* RFC 2828, 2017). Stallings e Brown (2018) definem o ataque como uma ameaça executada que, quando bem-sucedida, resulta em uma violação indesejável de segurança, sendo o responsável por sua execução denominado atacante ou agente fonte de ameaça.

Os ataques podem ocorrer por diferentes motivações, que vão desde interesses políticos e ganhos financeiros até o desejo de adquirir conhecimento sobre sistemas e tecnologia, em todos os casos, trata-se de ações intencionais, movidas por objetivos específicos, como extorsão, espionagem ou chantagem (Pinheiro, 2017).

Segundo Ferreira (2017), os ataques podem ser classificados em três categorias principais: internos, externos e físicos. Os ataques internos referem-se a incidentes originados por pessoas que atuam dentro da própria organização, por esse motivo, são considerados desenvolvidos internamente, podendo envolver o uso

indevido de credenciais, acesso não autorizado a informações ou sabotagem de sistemas. Os ataques externos ocorrem quando o invasor não possui permissão legítima para acessar a rede da organização e, por meio de técnicas fraudulentas ou da Internet, consegue obter acesso ao sistema. Já os ataques físicos envolvem o acesso direto ao espaço físico da empresa ou instituição, nesses casos, o invasor pode causar danos a equipamentos, modificar configurações críticas ou violar a confidencialidade de documentos e dispositivos.

1.10 Consequências Jurídicas para Empresas vítimas de Exploração Digital

Quando uma tentativa de ataque tem sucesso em seu propósito, seja ela interna ou externa, todos os dados mantidos por uma organização estão sujeitos à exposição, em especial as informações sigilosas de uma empresa, como planos de ação, questões financeiras, logs do sistema e dados sensíveis de seus clientes. Essas informações devem ser protegidas por uma série de procedimentos sugeridos pela LGPD e, quando isso não acontece, existem consequências legais que recaem sobre a empresa responsável pela segurança da informação.

Antes de abordar as obrigações legais de uma empresa referentes à proteção de dados, é necessário apresentar uma diferença fundamental entre dados pessoais e dados pessoais sensíveis. De acordo com Santos (2023), dados pessoais são descritos na LGPD como informações que podem identificar uma pessoa, independentemente do seu nível de detalhamento, incluindo o histórico de compras ou dados biométricos de um indivíduo.

Segundo a LGPD (Brasil, 2018), no Art. 5º para os fins desta lei, considera-se:

> I - Dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
>
> II - Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural

A administração de dados pessoais sensíveis exige que a empresa seja excepcionalmente rigorosa quanto à segurança e à confidencialidade dessas

informações, além de depender do conhecimento e da autorização dos titulares em relação ao uso desses dados, salvo quando houver previsão legal. Além dessas medidas, a lei também garante que o titular da informação não apenas tenha conhecimento sobre o uso de seus dados, mas possa rescindir o consentimento a qualquer momento (Santos, 2023).

Referente às consequências jurídicas a que as empresas estão submetidas em um cenário de exploração digital, estas podem ser divididas em duas formas de responsabilização: a responsabilidade civil e a responsabilidade administrativa.

Dentro da responsabilidade civil, existem duas modalidades: a subjetiva, que exige provas de que o causador do dano possua culpa, consciência e vontade de cometer a infração; e a objetiva, que não depende da culpa, sendo suficiente a confirmação do dano, no entanto, a LGPD não especifica qual modelo deve ser adotado (Caranti; Fukuhara, 2021).

Ao tratar da responsabilidade administrativa, analisa-se a importância do conhecimento sobre a legislação e da implementação de medidas efetivas que assegurem o cumprimento das regras de proteção de dados, pois, em casos de infração, a ANPD pode levar em consideração políticas claras, programas de *compliance* e boas práticas da empresa (Caranti; Fukuhara, 2021).

Segundo Santos (2023), no caso de um vazamento de dados em que os indivíduos possam correr riscos, a lei determina que os titulares dos dados confiados a uma empresa sejam comunicados, assim como a ANPD, que deve ser notificada dentro de um prazo determinado e informada detalhadamente sobre o incidente podendo incluir a natureza dos dados vazados, as medidas tomadas para resolver a questão e minimizar riscos.

Ainda no cenário de vazamento de dados, Santos (2023) enfatiza que um vazamento, por si só, não gera automaticamente o dever de indenizar por danos morais, sendo necessário, para tal, que o titular dos dados apresente provas concretas de prejuízos decorrentes dessa exposição.

1.11 Ataques de dia zero

As ameaças existentes aos sistemas de informação buscam explorar vulnerabilidades no *software*, que permitam abrir brechas para que o sistema seja completamente comprometido, resultando em acesso não autorizado, roubo de

dados, interrupção de serviços ou danos à integridade e à disponibilidade das informações, comprometendo, assim, a continuidade e a segurança operacional da organização. Dentre essas ameaças, existe uma que se aproveita do desconhecimento de vulnerabilidades presentes em *softwares*, permitindo que um sistema seja comprometido sem que haja, no momento, uma correção disponível, os quais são chamados de ataques *zero day*.

De acordo com Ali *et al*. (2022 *apud* Rocha, 2023), ataques de dia zero são ataques que exploram vulnerabilidades desconhecidas até então, o que representa uma séria ameaça para as organizações, pois costumam ser acompanhados por outros tipos de ataques, como vírus, cavalos de Tróia, *malware* e outras ameaças combinadas, com o objetivo de evitar a detecção por sistemas de segurança. Não existem muitas defesas contra esse tipo de ataque, pois, enquanto a falha permanece desconhecida, o *software* afetado não pode ser corrigido, e os antivírus não conseguem identificá-lo por meio da verificação de assinaturas.

Corroborando essa conceituação, o Google Threat Intelligence Group (GTIG) define ataques de dia zero como vulnerabilidades exploradas com fins maliciosos em ambientes reais antes que um *patch* seja disponibilizado publicamente (Charrier *et al*., 2025). Para os criminosos digitais, essas falhas não corrigidas em programas populares, como Microsoft Office ou Adobe Flash, são uma forma fácil de atacar qualquer alvo, desde grandes empresas até milhões de computadores pessoais ao redor do mundo (Bilge; Dumitras, 2012).

Quando um atacante identifica uma vulnerabilidade ainda desconhecida pelos desenvolvedores, ele desenvolve um *exploit*, isto é, um código ou técnica utilizada para explorar uma falha em um sistema. Geralmente, esse *exploit* é incorporado a um *malware* projetado especificamente para explorar a vulnerabilidade antes que os desenvolvedores a detectem. Somente após o ataque, a equipe responsável toma conhecimento da falha e inicia o processo de criação de uma correção para impedir a propagação do incidente (Lima, 2024).

De acordo com Guo (2022), estudos indicam que esses ataques representam uma das maiores ameaças à segurança da informação, uma vez que os métodos de detecção baseados em assinatura, isto é, impressões digitais que identificam um código malicioso, não são eficazes quando ainda não há registros dessas assinaturas.

Os ataques de dia zero permitem a exploração de outros tipos de ameaça a sistemas de informação, uma vez aberta uma brecha, os atacantes buscam explorar

o sistema utilizando diferentes tipos de ameaças, conforme a sua intenção, de modo que o ataque de dia zero se torna a porta de entrada para um comprometimento ainda maior do sistema.

De acordo com Guo (2023), em média, a cada 17 dias surge um novo ataque de dia zero, o que demonstra a frequência dessas ameaças no ambiente digital. O tempo médio para correção é de cerca de 15 dias, período em que os sistemas permanecem vulneráveis. Além disso, o custo médio de cada ataque pode chegar a milhões de dólares, evidenciando a gravidade dos impactos causados.

Pesquisas anteriores focaram em toda a janela de exposição de uma vulnerabilidade, que perdura até que todos os *hosts* vulneráveis sejam corrigidos. Essa janela inclui os ataques iniciados após a divulgação pública da falha, um estudo com três arquivos de *exploits* demonstrou que 15% deles foram criados antes da divulgação da vulnerabilidade correspondente. Outro estudo constatou que, no momento da divulgação, apenas 65% das vulnerabilidades em *softwares* de um *host* típico com Windows já possuíam *patches* disponíveis, o que oferece uma oportunidade para que invasores explorem falhas não corrigidas em larga escala (Bilge; Dumitras, 2012).

Um exemplo notório foi o *ransomware* WannaCry. O r*ansomware* é um tipo de *software* malicioso que impede o acesso a arquivos ou sistemas criptografando os dados, e exige o pagamento de um resgate em criptomoedas para que os dados sejam recuperados.

Segundo Moreira *et al*. (2017), o WannaCry era um *worm*, um *malware* que se replica com o objetivo de infectar outros computadores, que utilizava o *exploit* EternalBlue para explorar falhas no protocolo SMBv1 do Windows. Quando executado, tenta acessar dois domínios, caso obtenha sucesso, desliga-se automaticamente para evitar sistemas de análise. Em seguida, instalava-se como um serviço do sistema, copiando-se para as pastas do Windows e ativando o *ransomware* embutido, depois, busca baixar uma ferramenta para se conectar à rede Tor, uma rede anônima que oculta a identidade e a localização dos usuários, essa etapa fornece à vítima um endereço para pagamento em *bitcoin*, uma moeda digital descentralizada que permite transações anônimas, e uma chave para recuperação dos arquivos, mas essa parte do código não funciona devidamente. Por fim, o *worm* se espalha procurando computadores com a porta 445 aberta, tanto na rede local quanto em endereços IP aleatórios, para se infiltrar posteriormente. O exemplo do ransomware

WannaCry é uma dentre várias ameaças subsequente que o atacante pode explorar a partir de uma vulnerabilidade ainda não catalogada, fato esse, que evidencia o perigo potencial que os ataques de dia zero podem ocasionar em sistemas.

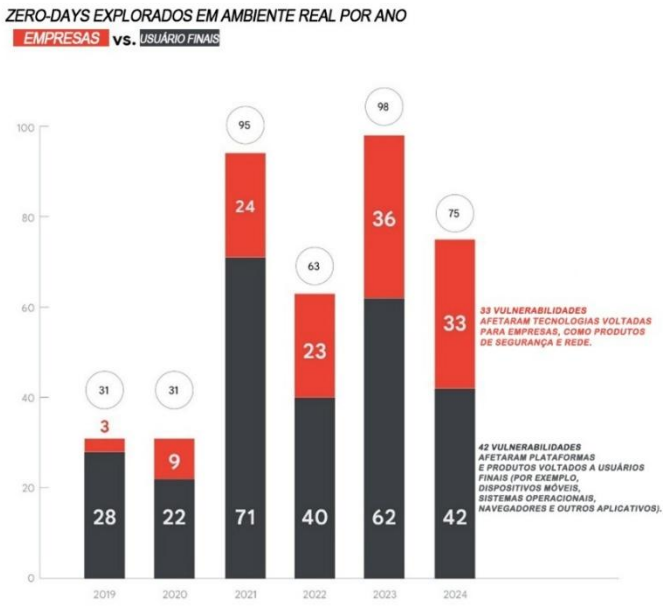
Para se ter uma estimativa, a equipe do Google Threat Intelligence Group realizou uma análise de exploração de ataques de dia zero em 2024, evidenciando fatores relevantes e marcantes presentes no relatório.

Segundo Charrier *et al*. (2025), redatores do relatório do Google Threat Intelligence Group (GTIG), foram rastreadas 75 vulnerabilidades de dia zero exploradas em 2024, número superior ao registrado em 2023 e 2022. As vulnerabilidades analisadas foram divididas em duas categorias principais: plataformas e produtos voltados a usuários finais, como dispositivos móveis, navegadores e sistemas operacionais e tecnologias destinadas a empresas, incluindo *softwares* e dispositivos de segurança.

Charrier *et al*. (2025), enfatizam que as explorações de dia zero vêm apresentando um número e variedade crescentes em relação a tecnologias corporativas, embora esse total ainda represente uma proporção menor quando comparado às tecnologias voltadas ao usuário final. Apesar do foco predominante em produtos populares para usuários finais, a tendência projetada é de um direcionamento cada vez maior para soluções empresariais, o que resultará em uma intensificação das medidas de segurança para reduzir futuras tentativas de exploração de dia zero.

A Figura 5, retirada do relatório *Hello 0-Days, My Old Friend: A 2024 Zero-Day Exploitation Analysis* representa a quantidade de detecção de vulnerabilidades de dia zero exploradas em 2024 em comparação aos anos anteriores, destacando um pico em 2021 e uma oscilação subsequente que, no entanto, não retornou aos valores mais baixos apresentados antes de 2021. Os autores destacam a melhoria contínua e a ubiquidade dos recursos de detecção, juntamente com divulgações públicas mais frequentes, como fatores que resultaram em números maiores de exploração de dia zero detectada em comparação ao observado antes de 2021.

Figura 5 – Quantidade de vulnerabilidades detectadas de dia zero



Fonte: Adaptado de Charrier *et al*. (2025).

Além disso, 44% das vulnerabilidades dos ataques de dia zero detectados em 2024 afetaram tecnologias corporativas, representando a maior média em proporção dentre todos os anos.

Conforme mencionado pelos autores Charrier *et al*. (2025) afirmam que o número de vulnerabilidades de dia zero exploradas em 2024 alcançou 75 ocorrências, seguindo uma tendência gradual de crescimento identificada nos últimos quatro anos. Embora as variações anuais oscilem, a média aponta para um crescimento lento, porém constante. O relatório destaca ainda que 44% dessas vulnerabilidades tiveram como alvo tecnologias corporativas, contra 37% em 2023, refletindo um aumento significativo, sobretudo em softwares e dispositivos de segurança e rede. As tecnologias corporativas, que representaram mais de 60% dos casos em 2024, demonstra uma preocupação crítica, pois sua exploração tende a gerar comprometimentos amplos de sistemas e redes.

Além disso, observa-se uma redução no número de explorações voltadas a navegadores e sistemas operacionais móveis, atribuída ao investimento crescente de fornecedores em técnicas de mitigação. Mais de 50% dos ataques de dia zero foram atribuídos a atores de espionagem cibernética, com destaque para grupos apoiados pela República Popular da China e pela Coreia do Norte, bem como clientes de fornecedores de vigilância comercial Charrier *et al.* (2025).

Portanto, os cenários desses ataques demonstram uma preocupação necessária para a segurança cibernética. Cada vez mais, sistemas são comprometidos decorrentes de vulnerabilidades ainda não divulgadas e corrigidas, permitindo que criminosos se beneficiem dessa porta, tanto no aspecto de usuários finais quanto, crescentemente, para as organizações, levando à preparação de medidas para detectar e prevenir esse tipo de ataque por parte dos agentes de ameaça.

1.12 Exemplo do caso MOVEit SQLi

Um exemplo recente de um caso que explorou uma vulnerabilidade ainda não conhecida foi o do caso MOVEit SQLi, uma solução empresarial para transferência segura e automatizada de arquivos entre usuários, sistemas e parceiros. Explorada em 2023, recebeu a identificação de CVE-2023-34362, do qual um grupo de *ransomware* chamado CL0P visava extorquir as vítimas através de exfiltração de dados.

A análise publicada pela Akamai Security Intelligence Group, conforme David *et al*. (2023, Figura 6), desenvolveu-se uma linha do tempo da exploração da vulnerabilidade. Em 31 de maio de 2023, a Progress Software, responsável pelos *softwares* MOVEit Transfer e pelo MOVEit Cloud, passou a informar seus clientes sobre uma vulnerabilidade de dia zero presente nesses sistemas, a qual estava sendo utilizada por agentes maliciosos para comprometer servidores expostos à Internet. Esse alerta foi emitido após a identificação de uma campanha de exploração que utilizava a falha para extrair arquivos confidenciais armazenados em servidores vulneráveis.

Conforme Mandiant (2023 *apud* David *et al*., 2023), as tentativas de exploração já vinham sendo observadas desde 27 de maio de 2023. Posteriormente, em 1º de junho de 2023, uma análise técnica elaborada pela Huntress confirmou que a vulnerabilidade possibilitava a execução remota de código no servidor.

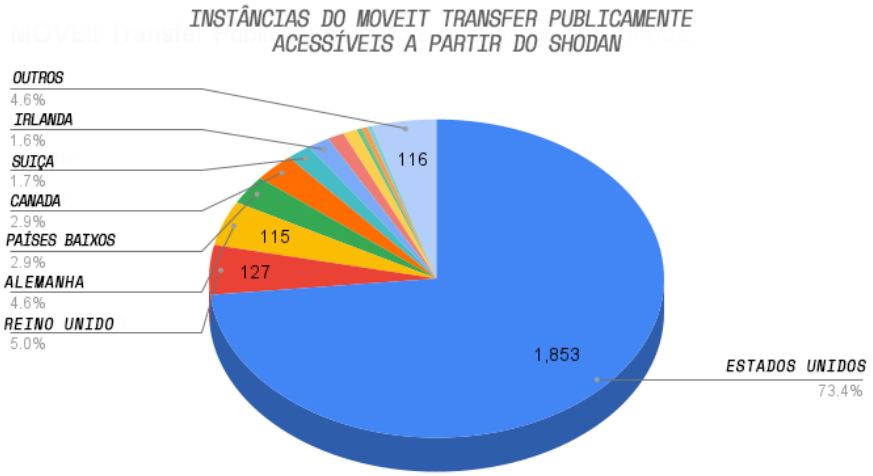
Figura 6 – Linha do tempo da exploração MOVEit

Fonte: David *et al*. (2023).

Ainda segundo David *et al*. (2023), em 2 de junho de 2023, a Microsoft atribuiu oficialmente a responsabilidade pelo ataque ao grupo Lace Tempest, fato este que foi posteriormente confirmada pelo grupo CL0P, por meio de uma declaração publicada em 5 de junho.

De acordo com Narang (2023, Figura 7), com base em uma consulta no Shodan, existiam 2.526 casos potencialmente vulneráveis do MOVEit Transfer acessíveis publicamente em 2 de junho de 2023. Os números, se dividiam em 73,4% nos Estados Unidos, Reino Unido com 5% e Alemanha com 4,6%. Além disso, países como Suíça, Canadá e Irlanda também apareciam na lista, juntamente com outros países não mencionados, que representavam uma parcela de 4,6% do total.

Figura 7 – Casos publicados pelo Shodan



Fonte: Tenable (2023) *apud* Narang (2023).

Como consequência, segundo Condon (2023), *patches* de correção foram divulgados pela Progress Software durante o mês de junho, no dia 7 de julho de 2023, foram divulgados oficialmente os três CVEs, contendo informações detalhadas sobre vulnerabilidades identificadas, juntamente com as respectivas correções, instruções de mitigações, versões atualizadas e métricas para avaliação de exposição de cada falha, por meio de verificações autenticadas para todos os clientes.

O caso MOVEit SQLi ilustra como vulnerabilidades desconhecidas podem ser exploradas de forma rápida, antes mesmo da disponibilização das correções. Esse cenário reforça a importância da adoção de estratégias eficazes de detecção e prevenção, capazes de mitigar ameaças de dia zero de maneira proativa.

1.13 Técnicas de Prevenção e Detecção de Ataques de Dia Zero

Após a compreensão dos fundamentos de segurança da informação, das vulnerabilidades e dos ataques de dia zero, torna-se essencial apresentar abordagens capazes de detectar e prevenir essas ameaças. Esta seção tem como objetivo expor as principais técnicas de detecção e prevenção de ataques de dia zero, com base em estudos recentes e práticas recomendadas. As técnicas descritas a seguir permitem tanto a identificação de ameaças ainda desconhecidas quanto a implementação de mecanismos que reduzem o risco de exploração.

1.13.1 Detecção de ataques de dia zero baseada em análise comportamental

O método de detecção baseada em análise comportamental, de acordo com Buckbee (2023), tem como finalidade identificar ataques de dia zero por meio de padrões de comportamento que indiquem o comprometimento de um sistema. Essa abordagem é amplamente utilizada em ferramentas de detecção e resposta de endpoints (EDR), que realizam o monitoramento contínuo de dispositivos e redes.

Como explicado por Buckbee (2023), a detecção de ameaças baseada em análise de comportamento opera com a definição de uma linha de base comportamental esperada, dessa forma, o monitoramento dos dados e comportamentos dos usuários na rede permite identificar anomalias que possam indicar a ocorrência de ataques. Ainda segundo o autor, essa abordagem considera os rastros deixados através de análises e averiguações dos dados dentro do sistema

e da rede. Comportamentos suspeitos, como tentativa de elevação de privilégio, movimentações anormais de arquivos e escaneamento de rede, são analisados e geram fortes indicativos de que um sistema pode ter sido comprometido.

Além disso, Buckbee (2023) complementa que comportamentos inesperados em processos ou aplicativos legítimos, como execução fora do padrão ou comunicação incomum com a rede, também devem ser considerados. Uma vez que um invasor consegue obter acesso às contas de usuários de dentro de um sistema, desvios comportamentais dessas contas, comparados com a linha de base comportamental esperada, podem alertar sobre uma possível violação do sistema. O monitoramento, portanto, possibilita a identificação de indícios de comprometimento de um sistema explorado por vulnerabilidades desconhecidas no momento do ataque, permitindo uma resposta rápida de segurança.

Esta forma de detecção se mostra eficaz, pois, de acordo com Kaspersky (2025), ferramentas EDR monitoram continuamente as informações em estações de trabalho e outros dispositivos, identificando violações de segurança em tempo real baseadas em comportamentos inesperados e desenvolvendo uma resposta rápida a possíveis ameaças. Uma análise de dados é realizada com o uso de aprendizado de máquina, que executa análises comportamentais sobre as informações coletadas, assim, qualquer atividade suspeita é reportada às partes interessadas.

1.13.2 Detecção de Ataques de Dia Zero utilizando inteligência artificial

A técnica de detecção abordado por Romar e Silva (2022), apresenta a inteligência artificial transformando os métodos de segurança digital, os quais passaram a utilizá-la, inclusive, na detecção de ataques de dia zero, constituindo uma alternativa viável e promissora para a segurança das informações, uma vez que a inteligência artificial permanece em constante aprendizado.

Segundo Romar e Silva (2022), o sistema EldeRan, desenvolvido por um grupo de pesquisadores britânicos, foi utilizado em experimentos voltados à identificação de *ransomwares* por meio de técnicas de inteligência artificial. O sistema parte da premissa de que *ransomwares* apresentam comportamentos distintos em relação a *softwares* legítimos, monitorando operações no sistema de arquivos, arquivos temporários e chamadas de API, interfaces que permitem a interação entre os diferentes componentes do sistema operacional. Após a coleta, os dados são

submetidos a um modelo de regressão logística regularizada, responsável por indicar se o programa analisado é legítimo ou malicioso.

Romar e Silva (2022) explicam que nos experimentos realizados, os pesquisadores britânicos compararam o desempenho do EldeRan com o antivírus VirusTotal. Foram utilizadas 942 amostras de *softwares* legítimos e 582 amostras de *ransomware*. O sistema EldeRan, segundo Romar e Silva (2022), apresentou uma taxa de detecção de 96,34% e falso positivo de 1,12%, enquanto o VirusTotal obteve 96,89% de detecção e 0,66% de falso positivo. Na etapa final, em que foram testadas categorias de *ransomware* desconhecidas simulando um cenário de ataque de dia zero, os pesquisadores concluíram que o EldeRan manteve um desempenho consistente, alcançando 93,3% de taxa de detecção.

De acordo com Romar e Silva (2022), os resultados demonstram que a aplicação de modelos de aprendizado de máquina oferece elevada precisão na identificação de comportamentos maliciosos, reforçando o potencial da inteligência artificial como ferramenta de defesa cibernética. Além disso, os autores destacam que os métodos baseados em assinaturas, tradicionalmente empregados em antivírus, tornaram-se menos eficazes diante da evolução das ameaças digitais. Dessa forma, a inteligência artificial representa uma tendência crescente para a detecção proativa de ataques de dia zero, capaz de antecipar padrões comportamentais incomuns e prever incidentes antes que causem danos significativos.

1.13.3 Detecção de ataques de dia zero baseado em análise de dados

O método de detecção baseado em análise de dados abordado pelos pesquisadores Bilge e Dumitras (2012) se baseia na comparação das datas de descoberta do ataque e da publicação da vulnerabilidade existente, permitindo um cruzamento de dados para identificar a possibilidade de um ataque de dia zero.

De acordo com Bilge e Dumitras (2012), é possível identificar ataques de dia zero a partir da criação de uma base de dados contendo informações sobre vulnerabilidades associadas a números de CVE, um padrão internacional usado para identificar e registrar falhas de segurança em *softwares*. Essa base inclui as datas de descoberta, divulgação e disponibilização de *patches*. Em seguida, essas vulnerabilidades são relacionadas aos *malwares* que as exploram, com base em dados públicos disponíveis em ferramentas como, por exemplo, o Threat Explorer da

Microsoft, que permite visualizar, investigar e monitorar em tempo real campanhas de *malware* e ameaças ativas em sistemas. Os arquivos maliciosos associados são então identificados a partir de registros de telemetria, consistindo na coleta automatizada de dados técnicos sobre o comportamento de arquivos, aplicativos e atividades suspeitas em dispositivos monitorados por antivírus.

Para aprofundar a análise, os pesquisadores explicam que, quando os *exploits* estão ocultos em arquivos não executáveis, como arquivos de texto, também são analisados os arquivos baixados logo após a exploração, a fim de complementar a investigação, uma vez coletados, os dados de reputação são utilizados para identificar a data de primeira aparição desses arquivos na Internet. Por fim, compara-se a data encontrada com a data de divulgação oficial da vulnerabilidade, caso o arquivo tenha sido detectado anteriormente, o incidente é classificado como um ataque de dia zero.

1.13.4 Prevenção de ataques de dia zero com arquitetura em Confiança Zero

De acordo com o guia explicativo da Microsoft (2025), o método de prevenção utilizando arquitetura de Confiança Zero opera em todos os recursos da organização por meio da autenticação contínua, sem presumir que qualquer usuário ou dispositivo seja confiável apenas por estar dentro do sistema, essa característica é essencial, pois estabelece uma vigilância permanente capaz de identificar e conter ameaças invisíveis. Um dos pilares, explica o guia, da Confiança Zero é o princípio de verificar previamente o acesso, antes de conceder qualquer permissão, o sistema analisa dados como identidade, localização, tipo de dispositivo e comportamento incomum.

A arquitetura de Confiança Zero atua em todos os recursos da organização por meio de autenticação contínua, evitando que qualquer acesso seja automaticamente considerado confiável, essa característica cria uma vigilância permanente capaz de identificar e conter ameaças ocultas. Essa checagem rigorosa impede que um *exploit* utilize credenciais roubadas ou acesse informações sensíveis, mesmo que o invasor ultrapasse uma camada de defesa, encontrará outras barreiras, pois cada nova solicitação de acesso exige uma validação adicional, isso reduz a possibilidade de movimentação lateral e aumenta as chances de detecção precoce de atividades fora do padrão. Parte do modelo baseia-se na suposição de violação, que recomenda a segmentação da rede e a aplicação de criptografia de ponta a ponta, ao dividir a rede em blocos menores e monitorá-los continuamente, qualquer tentativa de propagação

de um *exploit* pode ser rapidamente identificada como comportamento suspeito (Microsoft, 2025).

Dessa forma, conforme o guia explicativo da Microsoft (2025), quando um *exploit* tenta se autenticar utilizando credenciais roubadas, o sistema o bloqueia por meio de múltiplas camadas de verificação, impedindo que se aproprie de uma permissão no sistema, mesmo com credenciais corretas. Além disso, a segmentação de rede impede a movimentação lateral dentro da infraestrutura, pois cada segmento é monitorado e eventuais tentativas de deslocamento são detectadas como anomalias. Portanto, a arquitetura de Confiança Zero representa um modelo de segurança que, ao eliminar a confiança implícita e aplicar verificações contínuas, reduz drasticamente o risco de ataque e fortalece a defesa contra ameaças de dia zero.

1.13.5 Prevenção de ataques de dia zero com gerenciamento de *patches*

A técnica de prevenção através gerenciamento de *patches* consiste, segundo Koskenkorva (2021), em um monitoramento contínuo de vulnerabilidades e aplicação de *patches* conhecidos, reduzindo assim a janela de exposição, uma vez que muitos ataques ainda utilizam vulnerabilidades conhecidas.

Um processo de gerenciamento de *patches* deve contemplar a identificação contínua de vulnerabilidades em todos os ativos, além da avaliação do risco associado a cada falha, testes rigorosos dos *patches* em ambientes controlados e implantação planejada e monitorada das atualizações. A automação também é importante para garantir que *patches* sejam aplicados rapidamente e sem depender exclusivamente da aplicação manual, o que diminui o tempo em que sistemas ficam vulneráveis (Koskenkorva, 2021).

As orientações para planejamento de gerenciamento de *patches* apresentam que esse processo deve ser parte de uma manutenção preventiva dos ativos da informação, com o objetivo de evitar problemas de segurança, interrupções operacionais e perda de dados. Dessa forma, é fundamental a aplicação de *patches*, juntamente com o monitoramento contínuo, a fim de evitar que não sejam removidos ou não aplicados, aumentando a proteção contra ameaças de dia zero (NIST, 2022).

De forma complementar, Sangfor (2025) destaca que a classificação dos sistemas conforme seu grau de importância contribui para uma mitigação mais

eficiente, permitindo priorizar ações de correção com base na pontuação CVSS. Além disso, o autor ressalta a importância de avaliações regulares de vulnerabilidades e auditorias de segurança, práticas que fortalecem continuamente a postura defensiva das organizações e melhoram indiretamente a prevenção contra-ataques de dia zero.

Além disso, a NIST sugere que o gerenciamento de *patches* seja documentado detalhadamente, incluindo registro das vulnerabilidades, decisões de classificação de sistemas, datas de aplicação e resultados de verificação, esse registro permite auditorias futuras, identificação de lacunas no processo e aprimoramento contínuo das políticas de segurança.

1.13.6 Prevenção de ataques de dia zero com Windows Defender Exploit Guard

Outra abordagem de prevenção é o uso da ferramenta Windows Defender Exploit Guard (WDEG), desenvolvida pela Microsoft com o propósito de prevenir e detectar diferentes tipos de ataques cibernéticos, incluindo *malwares* tradicionais e avançados, *exploits*, *ransomware* e ataques baseados em rede. Segundo Kutsovsky (2017), gerente de programas da Microsoft, o WDEG foi introduzido na atualização Fall Creators Update do Windows 10, com o objetivo de reduzir pontos vulneráveis do sistema e bloquear comportamentos associados a ataques de *malware*.

O *software* é estruturado em quatro componentes principais: Redução da Superfície de Ataque (ASR), Proteção de Rede, Acesso Controlado a Pastas e Proteção contra Exploits. Cada um desses módulos atua em características específicas do sistema operacional, promovendo uma defesa abrangente que contribui diretamente para a prevenção de ataques de dia zero Kutsovsky (2017).

De acordo com Kutsovsky (2017), cada componente opera com uma característica própria de defesa: o conjunto ASR são controles que impedem a infecção do computador por *malwares*, bloqueando ameaças que utilizam os documentos do Office, scripts e em e-mails maliciosos. O segundo componente chamado Proteção de rede, protege o dispositivo final contra ameaças baseadas em web, bloqueando qualquer processo que interaja com hosts e IPs não confiáveis. O terceiro componente de segurança do Windows Defender Exploit Guard é o Acesso controlado a pastas, como o nome sugere, esse mecanismo de segurança protege dados confidenciais contra *ransomware*, bloqueando o acesso de processos maliciosos a pastas não protegidas. Por último, a Proteção contra *exploits* é um

conjunto de medida de mitigação de *exploits* que podem ser configuradas para defender o sistema e aplicativos.

Dentre esses recursos, destaca-se o ASR, Redução da Superfície de Ataque, pois como explicado por Kutsovsky (2017), ele fornece às empresas mecanismos de inteligência capazes de bloquear comportamentos utilizados por documentos maliciosos, evitando sua execução. Ao bloquear comportamentos suspeitos de forma preventiva, independente da ameaça ou exploração, o ASR protege ameaças de ataques de dia zero.

Ainda segundo Kutsovsky (2017), o ASR opera protegendo contra três principais vetores de ataque: aplicativos Office, scripts e e-mails. Nos aplicativos do Office, impede a criação de conteúdo executável, bloqueia a execução de processos filhos e de código de macro ofuscado, entre outros. Para scripts, ele bloqueia códigos maliciosos em JavaScript, VBScript e PowerShell, incluindo aqueles ofuscados ou baixados Internet. Em relação aos e-mails, o *software* bloqueia a execução de conteúdo executável extraído de *e-mails*.

Dessa forma, pode-se concluir que, o uso do Windows Defender Exploit Guard, com o apoio do ASR, permite neutralizar tentativas de exploração ainda não catalogadas com base em comportamentos maliciosos independentemente da ameaça ou exploração, tornando-o uma barreira eficiente contra-ataques de dia zero, a seção metodológica posterior irá descrever um laboratório prático que utiliza o software da Microsoft para prevenção contra esse tipo de ataque.

2 METODOLOGIA

Esta monografia foi desenvolvida com base em uma metodologia exploratória qualitativa, que, de acordo com Gil (2008), tem como principal função desenvolver, esclarecer e modificar conceitos e ideias, buscando formular problemas mais precisos ou hipóteses questionáveis para estudos posteriores.

Visando coletar e analisar dados relativos a medidas de detecção e prevenção de ataques de dia zero e demais conceitos relacionados à segurança da informação, a pesquisa foi realizada por meio de revisão bibliográfica, artigos científicos, publicações especializadas e fonte técnicas. Após a conclusão da fundamentação teórica, buscou-se obter uma compreensão geral dos conceitos de relevância na pesquisa, apresentação de um exemplo recente e da abordagem de técnicas de detecção e prevenção que respondessem o objetivo específico deste trabalho.

A escolha das técnicas aplicadas neste trabalho, sendo elas a detecção baseada em análise de dados e a prevenção utilizando o Windows Defender Exploit Guard, foi definida considerando fatores diretamente relacionados ao problema de pesquisa, à viabilidade prática do laboratório e à adequação dessas abordagens ao contexto dos ataques de dia zero. Dentre as técnicas de detecção apresentadas no referencial teórico, a análise de dados proposta por Bilge e Dumitraș (2012) mostrou-se mais apropriada, pois seu foco está justamente em identificar incidentes que ocorrem antes da publicação oficial de uma vulnerabilidade, permitindo diferenciar ataques comuns de ataques de dia zero por meio da correlação entre datas de descoberta, telemetria e reputação de arquivos. Além disso, essa técnica possibilita a reprodução do experimento em ambiente controlado sem a necessidade de grandes volumes de dados, modelos de aprendizado de máquina ou infraestrutura avançada, o que a torna mais compatível com o escopo deste trabalho. Outro ponto que reforça sua escolha é o fato de ela não depender de assinaturas previamente conhecidas, característica inadequada para lidar com ataques de dia zero, permitindo a análise de comportamento temporal e alterações de integridade mesmo na ausência de informações oficiais sobre o malware.

Da mesma forma, a técnica de prevenção selecionada, baseada no uso de regras de Redução de Superfície de Ataque (ASR), foi escolhida por se alinhar ao modo como muitos ataques de dia zero se manifestam na prática, utilizando scripts,

macros e execuções automatizadas para comprometer o sistema antes da existência de um patch. As regras ASR atuam justamente impedindo esse tipo de comportamento, bloqueando a execução suspeita mesmo quando a ameaça é inédita e ainda não foi catalogada. Essa característica torna o método adequado para o cenário de dia zero, já que a detecção não depende de assinaturas e sim da análise do comportamento do arquivo. Além disso, a aplicação das regras ASR em ambiente Windows permite demonstrar na prática como a prevenção ocorre, sem exigir arquiteturas mais complexas, possibilitando a realização do experimento em máquina isolada e garantindo a obtenção de logs e evidências necessárias para análise. Portanto, a combinação dessas duas técnicas foi escolhida por apresentar um equilíbrio entre relevância técnica, aplicabilidade prática e aderência ao objetivo central da pesquisa, permitindo tanto a demonstração teórica quanto a validação experimental do processo de detecção e prevenção de ataques de dia zero.

Um cenário simulado foi utilizado para exemplificar ambas, validando o conteúdo abordado e caracterizando a pesquisa com um caráter prático. Todos os experimentos foram desenvolvidos em ambiente controlado pelos autores, visando verificar a eficácia dos métodos selecionados. Os resultados foram detalhadamente analisados, seguindo corretamente as técnicas abordadas, garantindo que fossem replicáveis.

Todos os testes foram documentados e ilustrados com imagens, acompanhados de descrições detalhadas dos procedimentos e resultados, de modo a garantir clareza, repetição e transparência metodológica.

2.1 Seleção e Aplicação de Técnicas de Detecção e Prevenção de Ataques de Dia Zero

Com base nos conceitos apresentados no referencial teórico, esta seção apresenta as técnicas de detecção e prevenção de ataques de dia zero selecionadas para a etapa prática do estudo. Foram consideradas três abordagens de detecção, das quais são: análise comportamental, inteligência artificial e análise de dados. Juntamente com e três técnicas de prevenção, das quais são: arquitetura de confiança zero, gerenciamento de patches e vulnerabilidades e prevenção de ataques de dia zero com o uso do Windows Defender Exploit Guard. A partir dessa análise, foram escolhidas para aplicação prática a detecção baseada em análise de dados e a

prevenção utilizando o Windows Defender Exploit Guard, que serão explicadas e aplicadas no laboratório prático a seguir.

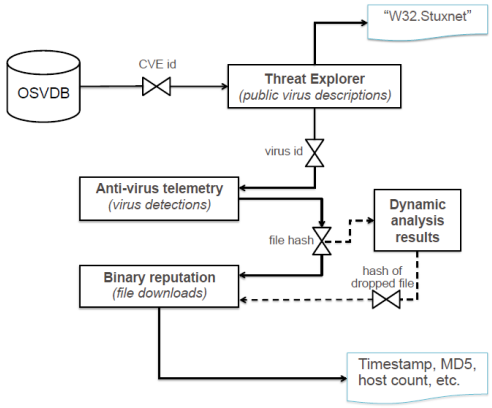
Essas técnicas foram selecionadas, pois utilizam diferentes sistemas operacionais, as quais demonstram um caráter abrangente do trabalho, juntamente com uma fácil replicação do experimento realizado. O sistema utilizado na detecção é o Linux, comumente empregado em servidores e voltado à identificação de ameaças, destacando-se pela disponibilidade de ferramentas gratuitas, de fácil instalação e operação, características que tornam sua aplicação acessível e eficiente em ambientes de pesquisa e teste

A técnica de prevenção demonstrada utiliza o sistema operacional Windows na sua versão 11, inevitavelmente devido ao uso de uma ferramenta nativa e exclusiva da Microsoft, o Windows Defender Exploit Guard utilizada na técnica. Essa escolha também contribui para a acessibilidade e aplicabilidade do estudo, uma vez que o Windows é amplamente utilizado por usuários finais e oferece recursos integrados voltadas à mitigação de *malwares* e ataques cibernéticos. Essas decisões metodológicas fundamentam a aplicação prática desenvolvida e detalhada nas próximas subseções.

2.2 Explicação do método de detecção

O método de detecção baseada em análise de dados foi um método desenvolvido pelos pesquisadores Bilge e Dumitras (2012), dos quais elaboraram um diagrama exemplificando o processo em cada uma das etapas (Bilge; Dumitras, 2012; Figura 8).

Figura 8– Método detecção de ataque dia zero



Fonte: Bilge e Dumitras (2012).

Conforme proposto por Bilge e Dumitras (2012), o método de análise para identificação de ataques de dia zero é dividido em cinco etapas principais: construção da base de dados inicial, identificação de *exploits* em executáveis, identificação de executáveis baixados após a exploração na qual é uma fase opcional, análise da presença de *exploits* na Internet e, por fim, decisão sobre se é um ataque de dia zero.

No primeiro momento, realiza-se a construção da base de dados inicial a partir de informações sobre vulnerabilidades conhecidas no sistema operacional escolhido e em softwares executados nesse sistema. Para isso, efetua-se uma busca no banco de dados sobre vulnerabilidades conhecidas, como o banco de vulnerabilidades OSVDB, ou em boletins técnicos, com o intuito de coletar dados sobre as vulnerabilidades divulgadas. Cada vulnerabilidade recebe um CVE ID do qual armazena informações sobre a data de descoberta, data da divulgação pública, data de lançamento do *exploit* e data do *patch* de correção.

Na sequência, essas vulnerabilidades são associadas às ameaças que as exploram, por meio de consultas em ferramentas de pesquisa e inteligência, como por exemplo o Symantec Threat Explorer, do qual fornece dados atualizados sobre ameaças e suas respectivas explorações. Cada ameaça recebe um rótulo chamado vírus ID que pode ser como um nome, como por exemplo W32.Stuxnet, mas também pode ser um identificador numérico.

Posteriormente, filtram-se os IDs de vírus que correspondem a detecções genéricas de vírus, por exemplo, um cavalo de tróia, de modo a manter apenas as detecções específicas que relacionam diretamente um vírus ID a uma vulnerabilidade

CVE. Esse processo resulta no mapeamento de ameaças e suas respectivas vulnerabilidades, constituindo os candidatos à análise de ataques de dia zero (Bilge; Dumitras, 2012).

Em um segundo momento, busca-se identificar os *exploits* detectados em executáveis associados em cada vírus ID. Para isso, são usados dados coletados pelos antivírus, chamados de telemetria, que registram os *hashes* de todos os arquivos maliciosos que eles encontram, o antivírus da Symantec é um exemplo que armazena dados de telemetria. Cada arquivo é identificado por um hash ID, é comum que um mesmo vírus ID esteja vinculado a diversos *hashes* de arquivo, devido às técnicas de polimorfismo, técnica que consiste em alterar pequenos detalhes do código para enganar os antivírus, empregadas por desenvolvedores de *malware* para dificultar a detecção. Assim, obtém-se um mapeamento entre a ameaça e as suas variantes, permitindo a análise da distribuição dos arquivos maliciosos (Bilge; Dumitras, 2012).

A etapa seguinte, considerada opcional, consiste na identificação de malwares que aparecem apenas após a execução de um *exploit*, geralmente embutido em um arquivo não executável, como um PDF. Nesses casos, o *exploit* realiza o download de um binário ou *payload* responsável pela ação maliciosa. Essa fase busca detectar arquivos baixados após a execução desses *exploits*, que podem não estar presentes no conjunto de dados de reputação binária. Embora essa abordagem amplie o escopo da análise, também pode gerar falsos positivos, pois o arquivo baixado pode ter origem legítima ou resultar de outro vetor de infecção não relacionado ao ataque de dia zero. Assim, essa etapa opcional requer investigação minunciosa para confirmar a relação causal entre *exploit* e *payload* (Bilge; Dumitras, 2012).

Na sequência, realiza-se a análise da presença dos *exploits* na Internet que consiste em analisar todos os binários baixados em hosts finais ao redor do mundo com o objetivo de estimar o momento em que cada arquivo executável foi detectado pela primeira vez em ambiente real. Os dados de reputação binária, utilizados nessa fase, indicam a ocorrência de um ataque, mas não necessariamente o sucesso da infecção. Assim, a primeira aparição de um determinado arquivo marca o início da atividade daquele ataque, permitindo aproximar o período de sua ocorrência. Nesta etapa também, obtém-se a data de *download*, o hash (MD5 e SHA256) do binário e a URL de onde foi baixado, entre esses arquivos podem estar binários maliciosos que

não foram detectados no momento do *download*, pois a ameaça ainda era desconhecida (Bilge; Dumitras, 2012).

Finalmente, para identificar os ataques de dia zero, compara-se a data de aparição de cada ataque juntamente com as datas de divulgação pública das vulnerabilidades correspondentes. Caso ao menos um dos *hashes* de arquivo de determinada ameaça tenha sido baixado antes da data de divulgação da CVE associada, conclui-se que a vulnerabilidade é do tipo de dia zero e que a ameaça correspondente executou um ataque de dia zero (Bilge; Dumitras, 2012).

2.2.1 Explicação do cenário

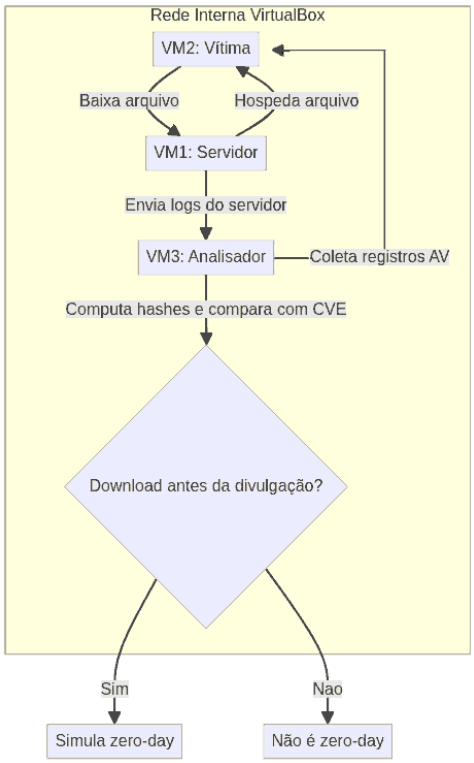
O cenário de teste preparado para simular o método de detecção baseado em análise de dados foi elaborado da seguinte forma: o laboratório utilizou o *software* de virtualização VirtualBox, no qual foram configuradas três máquinas virtuais em uma rede interna. A primeira máquina virtual atuou como servidor, a segunda como máquina vítima e a terceira como máquina analisadora.

Cada máquina assumiu um papel específico para simular uma infecção e, posteriormente, a detecção de uma exploração de dia zero. A VM servidor atuou como servidor HTTP, sendo responsável por hospedar os arquivos de teste e registrar os *logs* de acesso. A VM vítima representou um *host* final que realizou o *download* dos arquivos hospedados no servidor, todos os *downloads* foram registrados, simulando a atividade de um usuário comum em rede. A VM analisador executou o antivírus ClamAV, responsável por gerar a telemetria de segurança, e manteve um repositório de reputação binária para agregar *logs* e informações. O analisador foi o ponto central para a detecção e análise de ameaças, e o fluxo do processo prático está exemplificado na Figura 9.

O fluxo funcionará da seguinte forma: a VM servidor hospedará um arquivo que será baixado pela VM vítima, sendo este evento de *download* devidamente registrado. Na sequência, a VM analisador coleta os *logs* gerados pelo servidor, incluindo registros de acesso e *download*, assim como os registros de detecção do antivírus ClamAV provenientes da VM vítima. O VM analisador então computa os *hashes* dos arquivos baixados e os compara com uma data de divulgação fictícia de um CVE. Por fim, uma decisão é tomada com base na comparação se o *download* do arquivo pela vítima ocorreu antes da data de divulgação do CVE, isso simula um cenário de ataque

de dia zero, no qual a ameaça foi explorada antes de ser publicamente conhecida e, portanto, antes que as defesas pudessem ser atualizadas.

Figura 9- Fluxo do processo utilizado no laboratório



Fonte: Elaborado pelos autores (2025).

Caso o *download* tenha ocorrido após a data de divulgação, não foi considerado um ataque de dia zero, indicando que a vulnerabilidade já estava publicamente divulgada. As especificações de cada máquina virtual, incluindo o sistema operacional e os detalhes de *hardware*, estão demonstradas no Quadro 1.

Quadro 1 – Especificações de cada máquina virtual

VM	SO sugerido (livre)	RAM	CPUs	Disco (GB)
Servidor	Ubuntu Server 22.04 LTS	3 GB	3 CPU	10 GB
Vítima	Ubuntu Desktop 22.04	6 GB	4 CPU	20 GB
Analisador	Debian 12	4 GB	3 CPU	15 GB

Fonte: Elaborado pelos autores (2025).

O papel de cada máquina foi descrito da seguinte forma: a VM servidor atuou como servidor *HTTP*, sendo responsável por hospedar arquivos de teste e registrar *logs* de acesso, simulando a origem de potenciais ameaças. A VM vítima representou

um *host* final que realizou *downloads* de arquivos do servidor, e todos os *downloads* foram devidamente registrados, simulando a atividade de um usuário comum em rede. Por fim, a VM analisador conteve o antivírus ClamAV, que simulou a telemetria de segurança e um repositório de reputação binária. O analisador foi o ponto central do experimento. As especificações de rede das máquinas estão demonstradas no Quadro 2.

Quadro 2 – Configuração de Rede das máquinas virtuais

VM	IP Rede Experimento	Máscara Rede Experimento	Interface 2 Acesso Externo
Servidor	192.168.1.10	255.255.255.0	NAT
Vítima	192.168.1.20	255.255.255.0	NAT
Analisador	192.168.1.30	255.255.255.0	NAT

Fonte: Elaborado pelos autores (2025).

2.2.2 Preparação da máquina servidor

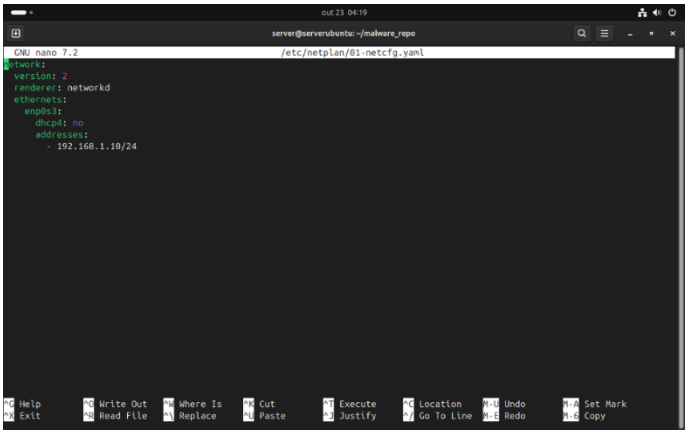
Para a VM servidor, cuja responsabilidade foi hospedar arquivos de teste e registrar acessos simulando a origem dos binários maliciosos, o sistema operacional utilizado foi *Ubuntu Server 22.04*, com um adaptador configurado na rede interna chamada rede experimento e outro adaptador em modo NAT para o *download* das ferramentas necessárias. Essa configuração repetiu-se em todas as máquinas do experimento.

Após a instalação do sistema operacional, foram aplicadas as configurações de rede destinadas à interface da rede interna, conforme especificado na tabela apresentada anteriormente. O arquivo responsável pelas definições de rede no Ubuntu localizou-se em `/etc/netplan/01-netcfg.yaml`. A Figura 10 apresenta esse arquivo.

O arquivo de configuração do *Netplan* iniciou com *network*, indicando a configuração de rede. Em seguida apresentou o número de versão, que definiu a versão do Netplan. A opção *renderer* indicou que o gerenciamento da rede foi realizado pelo *networkd*. Na seção *ethernets*, o nome enp0s3 referiu-se à interface de rede conectada à rede interna. A linha seguinte especificou que não foi utilizado *DHCP* para obter um endereço automaticamente. Logo abaixo a seção *addresses* definiu um

IP estático como 192.168.1.10/24 garantindo que a interface utilizasse sempre esse endereço com máscara de sub rede 255.255.255.0 de forma fixa.

Figura 10 – Configuração de rede

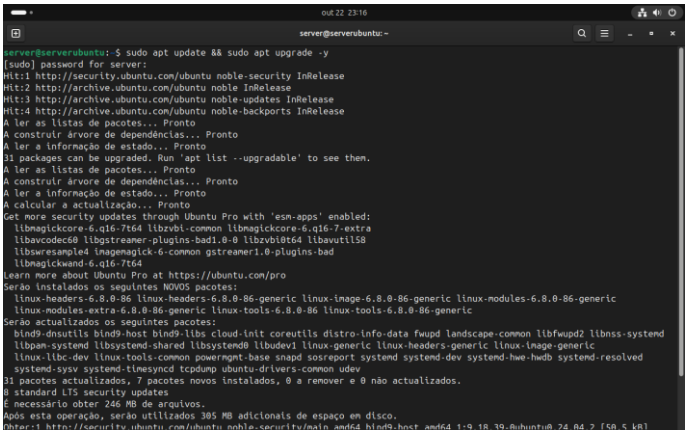


Fonte: Elaborado pelos autores (2025).

A etapa seguinte consistiu na atualização e instalação dos utilitários essenciais do sistema, procedimento para garantir que o ambiente estivesse preparado para a os experimentos. Para isso foram utilizados os comandos `sudo apt update && sudo apt upgrade -y` responsáveis por atualizar a lista de pacotes disponíveis nos repositórios e aplicar todas as atualizações pendentes do sistema operacional.

O parâmetro -y foi utilizado para confirmar automaticamente as instalações evitando a necessidade de confirmação manual durante o processo. Essa atualização assegurou que o sistema permanecesse na versão mais recente e com a lista de pacotes atualizada reduzindo riscos de incompatibilidade nas etapas seguintes da configuração. Além disso a atualização do ambiente contribuiu para a estabilidade geral do sistema e minimizou erros causados por dependências desatualizadas. A Figura 11 apresenta essa etapa.

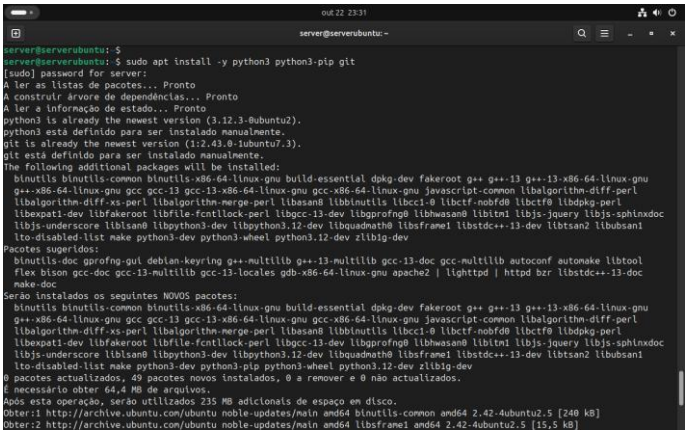
Figura 11 – Atualização da lista de pacotes



Fonte: Elaborado pelos autores (2025).

Na sequência o comando `sudo apt install -y python3 python3-pip git` foi executado para instalar o Python 3 o Pip e o Git. O Python 3 foi usado para disponibilizar um servidor HTTP simples que hospedou o arquivo de teste e registrou os *logs* de acesso da VM vítima. O Pip permitiu a disponibilização de instalação de bibliotecas auxiliares, caso fossem necessárias. O Git foi utilizado para baixar os arquivos do servidor simulando o comportamento de *download* da VM vítima a partir da Internet. A Figura 12 ilustra essa etapa.

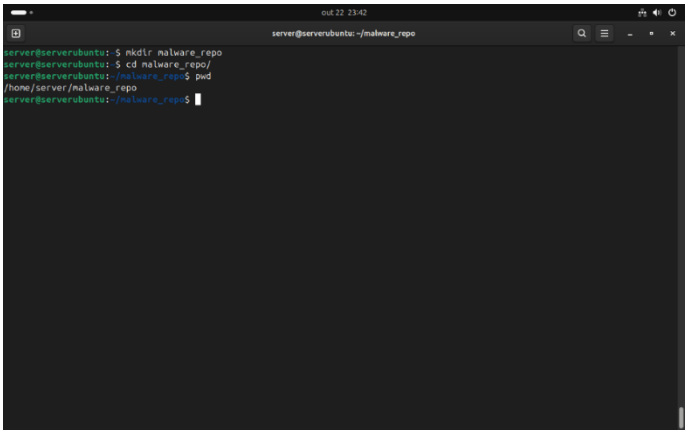
Figura 12 – Instalação das ferramentas



Fonte: Elaborado pelos autores (2025).

Após instaladas as ferramentas o diretório `malware_repo` foi criado na pasta *home* do usuário servidor onde foi armazenado o arquivo malicioso fictício para *download* posterior, conforme a Figura 13.

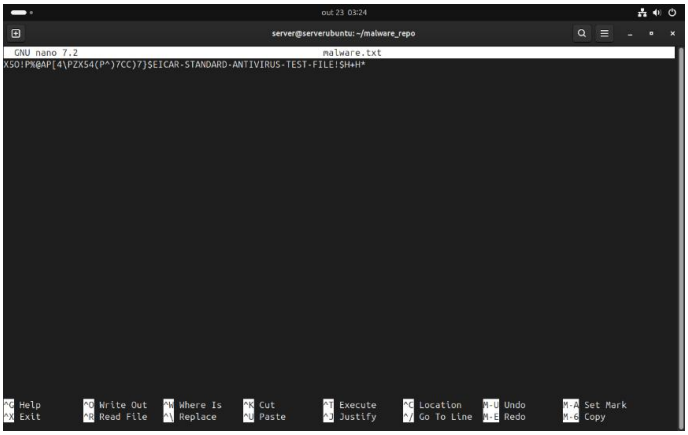
Figura 13 – Diretório do arquivo malicioso



Fonte: Elaborado pelos autores (2025).

A Figura 14 apresenta o arquivo `malware.txt` criado com a sequência EICAR utilizada para simular um arquivo malicioso de forma segura. O arquivo foi hospedado no diretório `malware_repo`, com o objetivo de servir como arquivo de teste para validação de antivírus no ambiente do laboratório. Dessa forma, foi possível validar o funcionamento do fluxo de coleta e análise de dados sem a utilização de códigos maliciosos reais garantindo a segurança e o controle do ambiente experimental.

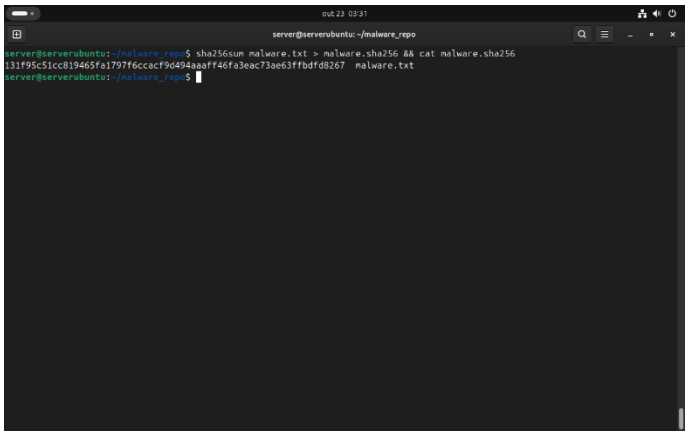
Figura 14 – Arquivo EICAR



Fonte: Elaborado pelos autores (2025).

Em seguida procedeu se ao cálculo do *hash* SHA256 deste arquivo utilizando o comando `sha256sum` no Ubuntu, onde o resultado foi salvo no arquivo `malware.sha256`. Esse *hash* foi necessário para identificar o arquivo de forma única. A Figura 15 exemplifica o comando junto do *hash* gerado do arquivo.

Figura 15 – Cálculo hash do arquivo malicioso

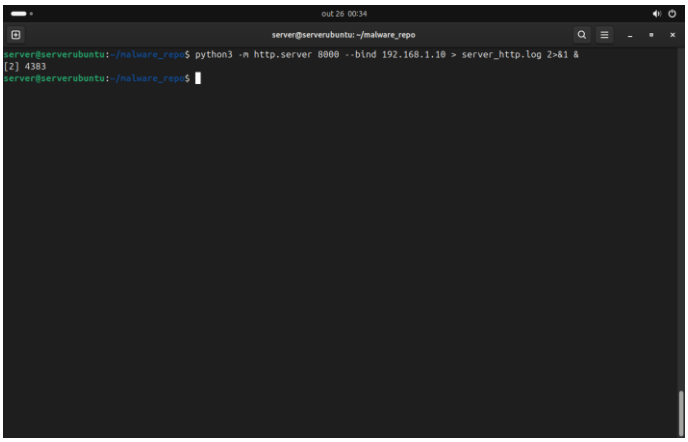


Fonte: Elaborado pelos autores (2025).

O passo seguinte foi a inicialização um servidor web simples com o protocolo HTTP utilizando Python, concomitantemente, em segundo plano, com o redirecionamento da saída padrão e de erro para o arquivo `server_http.log`. Este log foi usado para simular a reputação binária do arquivo. Para inicializar o servidor HTTP simples para a rede interna, o comando utilizado foi `python3 -m http.server 8000 --bind 192.168.1.10`, este comando indica que está sendo utilizado o interpretador Python na versão 3 com o parâmetro `-m http.server` que indica a execução de um módulo de servidor HTTP leve, configurado na porta 8000, este módulo vem embutido com a biblioteca padrão do Python. Por fim, o parâmetro –bind indica que o servidor operou apenas na interface de rede configurada na rede interna, permitindo que o arquivo seja acessado somente pelas máquinas do experimento.

Utilizou se o caractere de redirecionamento `>` para enviar a saída padrão para o arquivo `server_http.log` e a sequência `2>&1` para direcionar também o fluxo de erro padrão para o mesmo arquivo. Todo o comando foi executado em segundo plano indicado pelo `&`. A Figura 16 exemplifica o comando de inicialização do servidor HTTP acompanhado da configuração de redirecionamento de *log*.

Figura 16 – Habilitando servidor HTTP



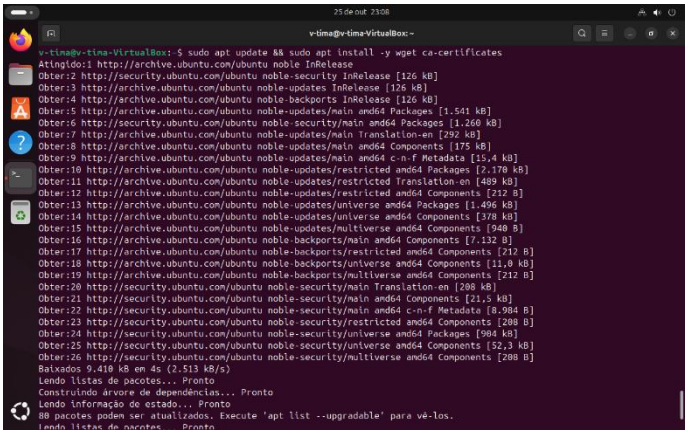
Fonte: Elaborado pelos autores (2025).

2.2.3 Preparação da máquina vítima

A preparação da máquina vítima teve como objetivo simular o comportamento de um usuário final que efetuou o *download* de arquivos da internet, neste caso foi baixado o arquivo de teste infectado com o vírus fictício. Assim como na máquina servidor, toda a configuração de rede estava exemplificada na tabela apresentada e os passos de configuração de rede na máquina seguiram os mesmos adotados na máquina servidor.

Com a máquina configurada, o primeiro passo foi atualizar a lista de pacotes e instalar os pacotes *wget* e ca-certificates. O pacote *wget* atua como utilitário de linha de comando para baixar arquivos via HTTP, HTTPS e FTP e teve a função de obter o arquivo de teste simulado infectado hospedado no servidor. O pacote *ca-certificates* foi necessário para a instalação e atualização de *softwares* de forma segura, pois reúne certificados raiz de autoridades certificadoras que emitem certificados digitais para websites e servidores. Sua importância neste exemplo residiu em permitir instalações seguras e em garantir que a segurança estivesse presente antes de realizar o *download*, destacando a necessidade de certificados atualizados para operações de rede. Como observação, o pacote *ca-certificates* estava presente nas demais máquinas do experimento, pois ele foi instalado automaticamente ao instalar o pacote *python3* ou o pacote *git*. O comando utilizado foi `sudo apt update && sudo apt install -y wget ca-certificates`, que atualizou a lista de pacotes e instalou os pacotes necessários, conforme retratado na Figura 17.

Figura 17 – Preparação dos pacotes

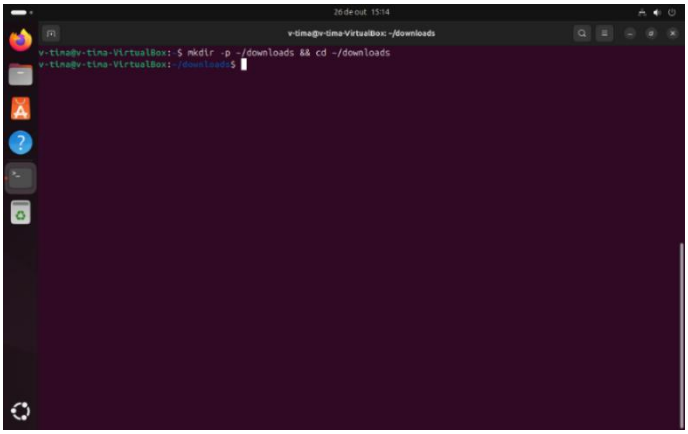


Fonte: Elaborado pelos autores (2025).

Após a instalação foi criado o diretório *downloads* dentro do diretório *home* da máquina vítima e foi definido como local de trabalho para as operações seguintes. Para isso foi executado o comando `mkdir -p ~/downloads && cd ~/downloads`.

O utilitário `mkdir` com a opção `-p` garantiu que o comando não falhasse caso o diretório já existisse e o operador `&&` assegurou que o `cd` só fosse executado se a criação tivesse sido bem-sucedida. A organização em um diretório dedicado simplificou a captura de informações e a coleta de logs referentes às operações de *download*. A escolha pela criação de um diretório para as operações, contribuiu para manter o cenário de teste replicável após a conclusão das atividades, simulando o local onde um usuário salvaria um arquivo baixado, conforme ilustrado na Figura 18.

Figura 18 – Criação do diretório de trabalho



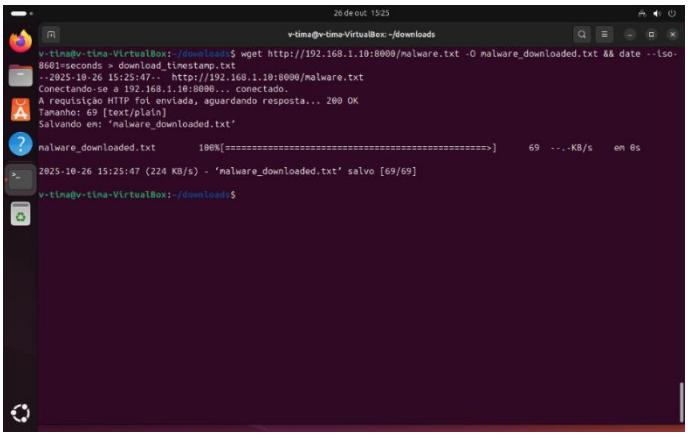
Fonte: Elaborado pelos autores (2025).

O *download* do arquivo e o registro de tempo foram realizados com o utilitário de linha de comando *wget*, que baixou o arquivo `malware.txt` hospedado no servidor HTTP da máquina servidor. Em paralelo foi executado o comando *date* com o parâmetro `--iso-8601=seconds` para gerar um *timestamp* que marcou o momento exato da execução do *download*. Esse padrão de tempo segue o formato ISO 8601.

O formato ISO 8601 organiza os registros de tempo na ordem de ano mês dia hora minutos segundos e milésimos. Por exemplo a data 27 de setembro de 2022 às 18 horas foi representada como 2022-09-27 18:00:00.000. A utilização desse formato pelo comando *date* permitiu registrar de modo padronizado a data e a hora do *download* pela máquina vítima, informação que será empregada no processo de reputação binária para identificar a origem da primeira ocorrência do arquivo.

Para efetuar o *download* foi executado o comando `wget http://192.168.1.10:8000/malware.txt -O malware_downloaded.txt` em que a primeira parte corresponde à URL do servidor interno incluindo a porta 8000 e o parâmetro `-O` salvou o arquivo baixado com o nome `malware_downloaded.txt` no diretório atual. Em seguida o comando `date --iso-8601=seconds > download_timestamp.txt` gerou o *timestamp* no formato ISO 8601 e salvou o resultado em *download_timestamp.txt*, conforme ilustrado na Figura 19.

Figura 19 – Download no arquivo malicioso

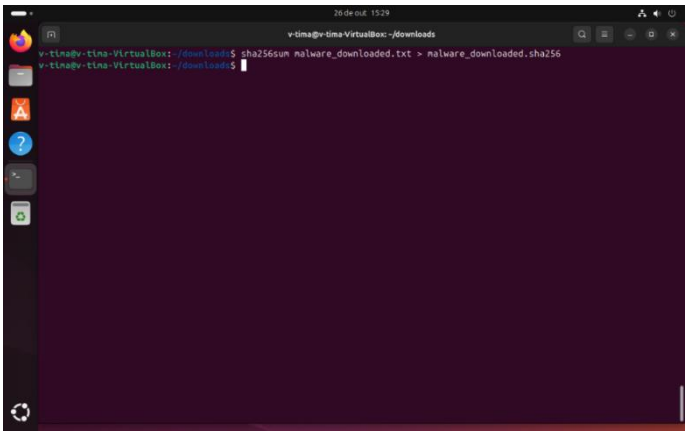


Fonte: Elaborado pelos autores (2025).

A geração do *hash* único foi realizada, utilizando o algoritmo criptográfico SHA256 aplicado ao arquivo recém baixado. O propósito desta etapa foi utilizar o *hash* como elemento da telemetria, permitindo que a máquina analisadora associasse o

arquivo alvo da infecção à detecção do antivírus e à reputação binária. Para isso foi executado o comando `sha256 summalware_downloaded.txt > malware_downloaded. sha256`, cuja saída foi salva em um novo arquivo contendo o valor SHA256 do arquivo analisado, conforme descrito na Figura 20.

Figura 20 – Hash do arquivo malicioso

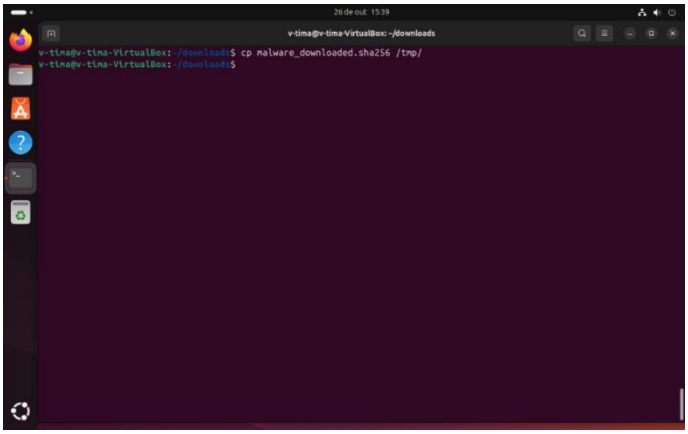


Fonte: Elaborado pelos autores (2025).

Por último, conforme a Figura 21, a máquina vítima gerou uma cópia do arquivo contendo o *hash* no diretório temporário do sistema usando o utilitário *cp*. O comando `cp malware_downloaded.sha256 /tmp/` indicou o arquivo de origem e o diretório de destino, onde foi salvo o arquivo, o resultado foi a criação da cópia no diretório *tmp* do sistema.

Esse procedimento foi adotado, porque o diretório temporário do sistema é um local de fácil acesso e comumente utilizado para transferência de arquivos por meios remotos, como *scp* ou pastas compartilhadas. Ao disponibilizar o *hash* do arquivo nesse diretório, a máquina vítima simulou a entrega dos dados de telemetria para a máquina analisadora, para posteriormente iniciar a etapa de análise.

Figura 21 – Cópia do arquivo hash para o diretório tmp



Fonte: Elaborado pelos autores (2025).

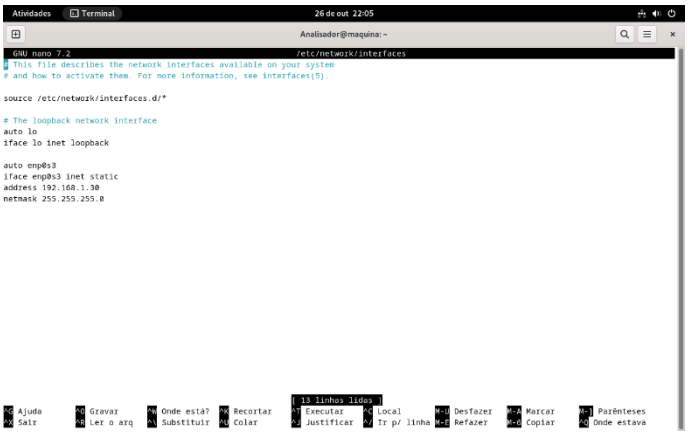
2.2.4 Preparação da máquina analisador

A VM analisador foi máquina central para análise, onde foram coletados os dados, realizada a simulação e a detecção do antivírus e executado o processo de reputação binária, além de efetuada a comparação final para identificar se se tratava de um ataque do tipo dia zero. Na VM analisador, diferentemente da máquina vítima, o passo relativo à configuração de rede foi demonstrado por se ter utilizado a distribuição Debian, diferente do Ubuntu empregado nas máquinas anteriores.

O primeiro passo foi a configuração da interface para que fosse permitido a comunicação com a rede interna do experimento, para isso, o arquivo de configuração utilizado no debian, localizou-se em `/etc/network/interfaces`.

A linha `auto enp0s3` definiu que a interface enp0s3 seria ativada automaticamente na inicialização do sistema. Logo abaixo, a instrução `iface enp0s3 inet static` determinou que a interface enp0s3 utilizaria uma configuração manual de IP. O identificador inet especificou o uso de um endereço IPv4. Por fim, as linhas `address` e `netmask` definiram o endereço de IP e a máscara atribuídos à interface, conforme ilustrado na Figura 22.

Figura 22 – Configuração de rede interna

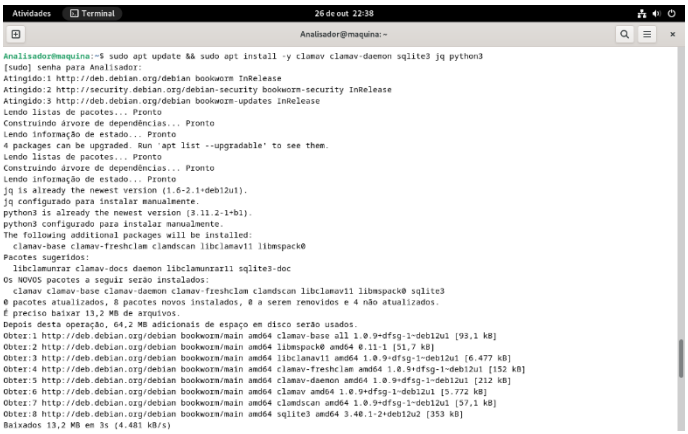


Fonte: Elaborado pelos autores (2025).

A próxima etapa constituiu na atualização da lista de pacotes junto com instalação dos softwares necessários para o analisador processar os dados coletados. Foram instalados os pacotes *clamav* e clamav-daemon, *sqlite3*, *jq* e *python3.*

Os pacotes *clamav* e *clamav-daemon* forneceram o antivírus ClamAV e seu serviço de fundo *daemon*, usados para simular a detecção de malware e gerar telemetria. Já os pacotes *sqlite3*, *jq* e *python3* não foram utilizados diretamente nesta demonstração, sendo incluídos apenas para ilustrar como o ambiente poderia ser expandido em um cenário real de análise, no qual o uso dessas ferramentas seria essencial para o tratamento, estruturação e processamento de grandes volumes de dados. A Figura 23 apresenta essa etapa de configuração

Figura 23 – Instalação de ferramentas



Fonte: Elaborado pelos autores (2025).

Com a etapa anterior concluída, foram executados os comandos necessários para atualizar as definições de vírus e inicializar os serviços do antivírus ClamAV. As instruções utilizadas foram `sudo freshclam || true`, na sequência `sudo systemctl start clamav-freshclam.service || true` e por último `sudo systemctl restart clamav-daemon.service`.

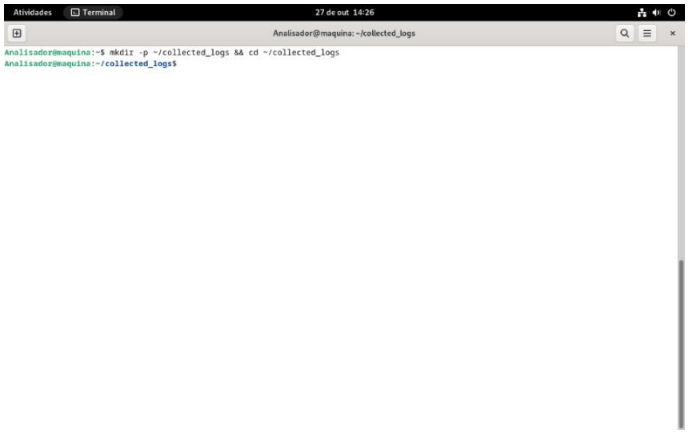
O primeiro comando realizou a atualização das assinaturas de vírus utilizadas pelo ClamAV, utilizando o utilitário *freshclam*. O operador `||` true garantiu que, caso ocorresse algum erro durante a atualização, o processo não fosse interrompido. Em seguida, o comando responsável por iniciar o serviço de atualização automática, `clamav-freshclam.service`, foi executado para manter as definições do antivírus atualizadas. Por fim, o serviço principal de varredura, `clamav-daemon`, foi reiniciado com o comando `systemctl restart`, assegurando que o ClamAV estivesse pronto para as próximas etapas de detecção e análise. A Figura 24 ilustra essa sequência de comandos.

Figura 24 – Configurações complementais do ClamAV

Fonte: Elaborado pelos autores (2025).

A etapa seguinte, foi a coleta dos arquivos hash do servidor e da máquina vítima para posteriormente serem utilizado na telemetria e na reputação binária. Para isso, inicialmente foi criado o diretório `collected_logs` no diretório *home* do usuário analisador, onde seriam armazenados os arquivos baixados do servidor e da vítima, conforme a Figura 25.

Figura 25 – Criação do diretório de arquivos para análise



Fonte: Elaborado pelos autores (2025).

Na etapa seguinte, foi necessária a instalação do pacote *openssh-server*, responsável por permitir a transferência de arquivos de forma segura pela rede interna. Essa instalação foi realizada em todas as máquinas do experimento para possibilitar a comunicação segura entre elas. Utilizou-se o gerenciador de pacotes *apt* com o comando `apt install openssh-server`. Esta etapa não foi ilustrada por não apresentar relevância visual para o experimento, uma vez que segue o mesmo procedimento de instalação já aplicado a outros pacotes.

Com o servidor *openssh* instalado em todas as máquinas, a transferência foi realizada através do utilitário *scp*, que opera na transferência segura de arquivos via criptografia pelo protocolo SSH. A operação consistiu em copiar o arquivo de *hash* da máquina vítima para a máquina analisador.

A estrutura do comando foi `scpvtima@192.168.1.20:/home/vtima/downloads/malware_downloaded.sha256 /home/Analisador/collected_logs`, operou na coleta do arquivo *hash* baixado da máquina vítima para a máquina analisador juntamente com os arquivos de *logs* da máquina servidor. O primeiro termo *scp* realizou a cópia via SSH, em seguida foi indicado o usuário e o endereço da máquina alvo, depois o caminho remoto do arquivo na máquina vítima e por fim o diretório local da máquina analisador onde o arquivo foi salvo. Esse procedimento permitiu a coleta do identificador de *hash* e dos arquivos de log necessários para a análise, conforme representado na Figura 26.

Figura 26 – Transferência de arquivo

Fonte: Elaborado pelos autores (2025).

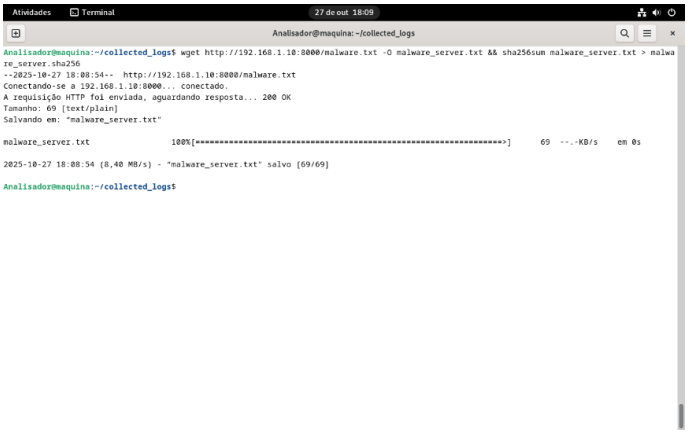
Com o arquivo de log do servidor, realizou-se a cópia para a máquina analisador usando o comando `scp server@192.168.1.10:/home/server/malware_repo/server_http.log /home/Analisador/ server_http.log`, conforme retratado na figura 27.

Figura 27 – Transferência de log

Fonte: Elaborado pelos autores (2025).

Para o arquivo malicioso utilizou se o *wget* para baixar uma cópia do arquivo original. Em seguida foi calculado o *hash* SHA256 sobre o arquivo copiado para posterior comparação, conforme ilustrado na Figura 28.

Figura 28 – Download do arquivo malicioso



Fonte: Elaborado pelos autores (2025).

2.3 Explicação do método de prevenção

O método de prevenção utilizando o ASR do Windows Defender Exploit Guard baseia-se na detecção comportamental, diferindo do método de assinatura empregada pelos antivírus tradicionais. O ASR atua em três vertentes principais*: e-mails*, aplicativos do Office e *exploits*. No caso dos aplicativos do Microsoft Office, o suporte nativo ao ASR foi introduzido apenas a partir das versões de 2021, razão pela qual o experimento utilizou o Office 365, compatível com as políticas de bloqueio comportamental aplicadas por esse recurso.

Segundo Kutsovsky (2017), os e-mails e aplicativos do Office são considerados fundamental para a produtividade, porém são os vetores mais comuns de ataque e podem causar grandes problemas para administradores de segurança, tanto o Office quanto o e-mail servem como meio simples e fácil para que agentes maliciosos lancem *malware* e ataques sem arquivo, embora a utilização de macros e *scripts* do Office se tornaram muito útil para produtividade, agentes maliciosos podem usá-los para executar exploits diretamente, de forma a operar inteiramente na memória e muitas vezes não são indetectáveis por técnicas antivírus tradicionais. Dessa forma, o ASR fornece inteligência integrada que bloqueia os comportamentos necessários usados por esses documentos maliciosos para serem executados, com isso, impedindo também, ataques de dia zero nunca vistos.

Kutsovsky (2017) continua abordando a capacidade de ASR bloquear também usuárias em relação a *exploits* emergentes, como era o DDEDownloader, do qual, utilizava o pop-up de Troca Dinâmica de Dados em documentos do Office para

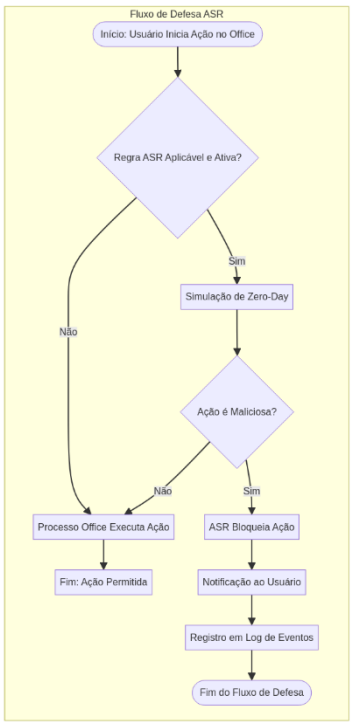
executar um *downloader* em PowerShell, no entanto, ao fazer isso, ele iniciava um processo filho que a regra correspondente em ASR bloqueava. Além disso, em relação a *scripts*, o ASR sofre um processo de treinamento constante em serviços de proteção em nuvem pela Microsoft para determinar se um *script* foi utilizado ou camuflado para fins maliciosos, de forma que, ao constatar uma alta correspondência, qualquer tentativa de acesso ao *script* é bloqueada.

Por último, mesmo com políticas em *e-mails* para limitar os arquivos que podem ser entregues às caixas de entrada de usuários, ainda assim, não há controle sobre os arquivos entregues por *e-mail* em dispositivos pessoais. Nesse escopo que o ASR também opera, permitindo que sejam aplicadas políticas de arquivos em *e-mails* pessoais, tanto para webmail quanto para clientes de *e-mail* em dispositivos empresariais. Por fim, O ASR depende de o Windows Defender Antivirus ser o antivírus principal no sistema em execução e de seu recurso de proteção em tempo real estar ativado Kutsovsky (2017).

2.3.1 Explicação do cenário

Para esse laboratório, foi utilizado o pacote Office como potencial vetor de ameaça, por meio do aplicativo Word que simulou a execução de um arquivo malicioso para exemplificar o bloqueio ASR. Na prática foi empregado um *exploit* fictício que, na realidade, consistiu em uma *macro* no Word responsável por criar um executável *.exe* apenas para demonstrar a ação de proteção. O mecanismo bloqueou a tentativa de execução independentemente de o *exploit* ser conhecido ou não. Esse processo neutralizou a fase final do *exploit*, pois, mesmo que a vulnerabilidade tivesse sido explorada, a infecção não foi concluída uma vez que o ASR impediu o comportamento subsequente necessário. Dessa forma o uso do Windows Defender Exploit Guard por meio do componente ASR permitiu demonstrar a prevenção de tentativas de exploração ainda não catalogadas, funcionando sobre o comportamento do ataque em vez da assinatura da ameaça. O fluxo do processo do laboratório prático está exemplificado na Figura 29

Figura 29 – Fluxo do processo de prevenção com ASR



Fonte: Elaborado pelos autores (2025).

O diagrama retrata a operação da defesa Attack Surface Reduction (ASR) no Office, detalhando o processo de decisão que ocorre a partir de uma ação do usuário.

A primeira etapa é o ponto de partida, quando o usuário realiza a ação no aplicativo Office, como, por exemplo, abrir um documento do Word que contenha um macro. Essa ação desencadeia uma sequência de eventos que pode levar a uma ação legítima ou a uma tentativa de ataque.

Na segunda etapa ocorre a verificação de uma regra ASR aplicável e ativa para o tipo de ação executada. Nesta etapa, o sistema determina se o mecanismo de defesa comportamental está em funcionamento para aquela situação específica. Se a regra ASR não estiver aplicável ou ativa, o fluxo segue para a execução normal da ação pelo Processo Office, finalizando em Ação Permitida.

Se a regra ASR estiver aplicável e ativa, a ação passa para a terceira etapa, que é o processo de decisão onde o ASR avalia o comportamento da ação. Este é o cerne da prevenção, pois o ASR não verifica a assinatura do arquivo, mas sim o comportamento que o aplicativo Office está tentando realizar, como a criação de um arquivo executável. Se a ação for considerada legítima, ela é liberada e o processo continua normalmente. Porém, se o comportamento for identificado como malicioso,

o ASR aciona o bloqueio, interrompendo a cadeia de ataque e impedindo que a ameaça se concretize.

Na quarta etapa ocorre a notificação do usuário, momento em que o ASR informa o bloqueio e fornece *feedback* imediato sobre a ação preventiva. Em seguida, na quinta etapa, o ASR registra o evento de bloqueio em *logs*, criando um registro de auditoria e evidência de que a defesa funcionou corretamente. Essas duas etapas encerram o fluxo de defesa. As especificações da máquina utilizada estão descritas no Quadro 4.

Quadro 3 – Especificações da máquina utilizada

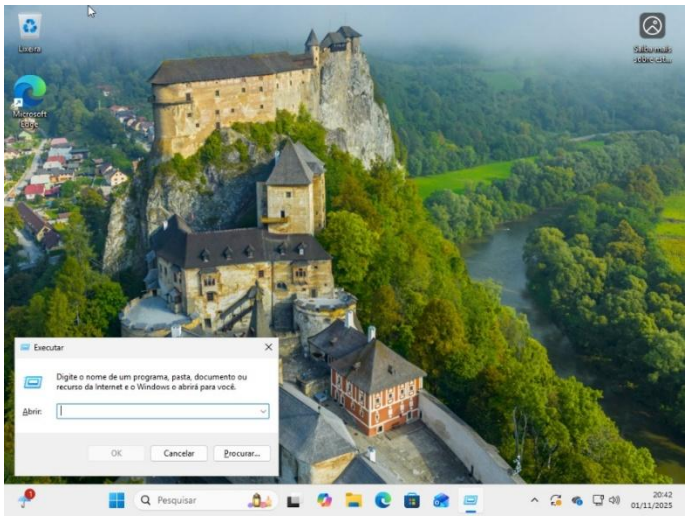
VM	SO Utilizado	RAM	CPUs		Disco (GB)
Experimento	Windows 11	12	5 CPU		80 GB

Fonte: Elaborado pelos autores (2025).

2.3.2 Preparação da máquina Windows

O primeiro passo para simular a prevenção por meio do ASR foi verificar se o usuário possuía privilégios de administrador. Essa verificação foi necessária porque os comandos do PowerShell utilizados alteram políticas de segurança centrais do sistema operacional Windows, em especial as configurações do Microsoft Defender. Para realizar a verificação de permissões no Windows 11, abriu-se o *Executar* pelo menu *Iniciar* ou por meio do atalho *Windows* + *R*, conforme ilustrado na Figura 30.

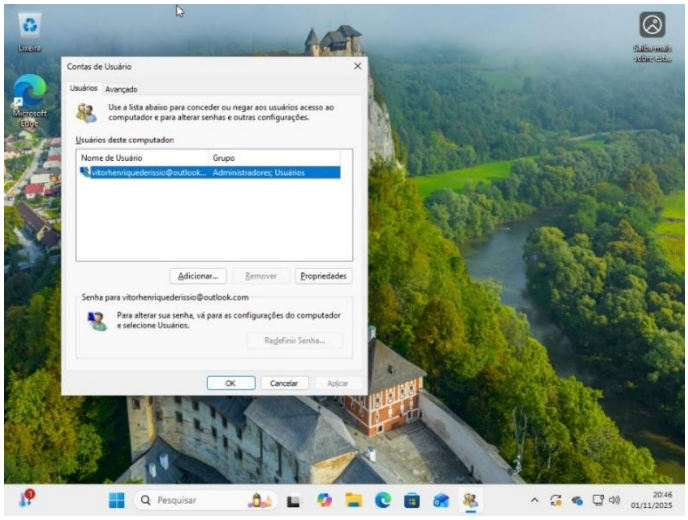
Figura 30 – Acessando o executar no Windows 11



Fonte: Elaborado pelos autores (2025).

O passo seguinte foi acessar o painel de contas de usuário digitando `control userpasswords2` na barra de pesquisa do *Executar*. Em seguida, o painel de contas de usuário foi exibido, mostrando os usuários cadastrados no sistema, conforme representado na Figura 31.

Figura 31 – Painel contas de usuário

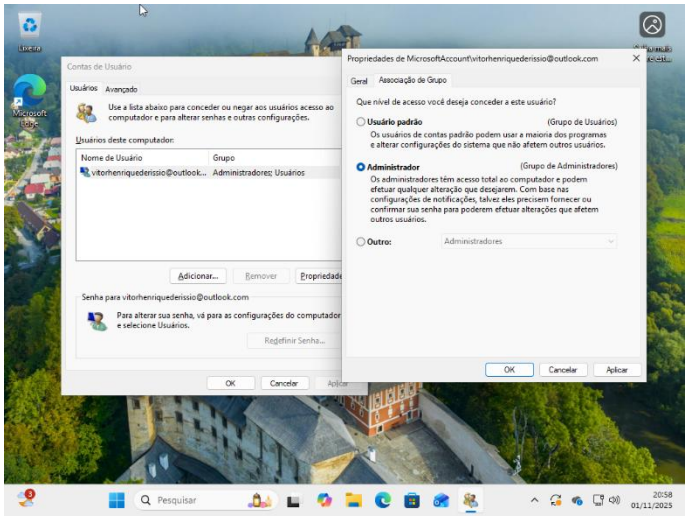


Fonte: Elaborado pelos autores (2025).

Na sequência, foi escolhido o usuário do sistema ao qual se desejava conceder permissões de administrador, neste caso, o único usuário criado para o experimento. Após a seleção, foram dados dois cliques sobre o usuário para abrir as configurações de permissões correspondentes. Na janela exibida, selecionou-se a guia *Associação*

em Grupo para acessar as opções de permissões, marcando-se a opção *Administradores* para conceder privilégios administrativos ao usuário. Por fim, para confirmar as alterações, clicou-se em *Aplicar* e em *OK*, salvando as mudanças, conforme ilustrado na Figura 36.

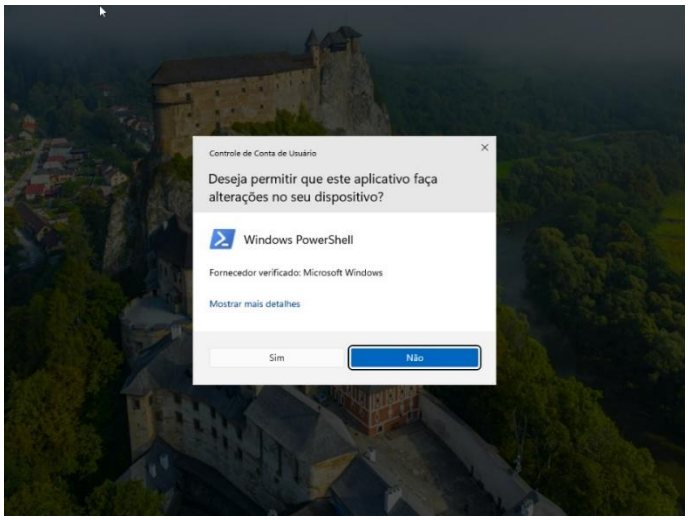
Figura 32 – Aplicação das permissões de administrador



Fonte: Elaborado pelos autores (2025).

Na etapa seguinte, foi necessário verificar se o ASR estava ativo e identificar quais regras estavam configuradas. Para isso, utilizou-se o PowerShell com privilégios de administrador. Assim como na etapa anterior, abriu-se o *Executar* e digitou-se PowerShell na caixa de pesquisa. Em seguida, pressionou-se *Ctrl* + *Shift* + *Enter* para iniciá-lo diretamente com privilégios de administrador, conforme ilustrado na Figura 33.

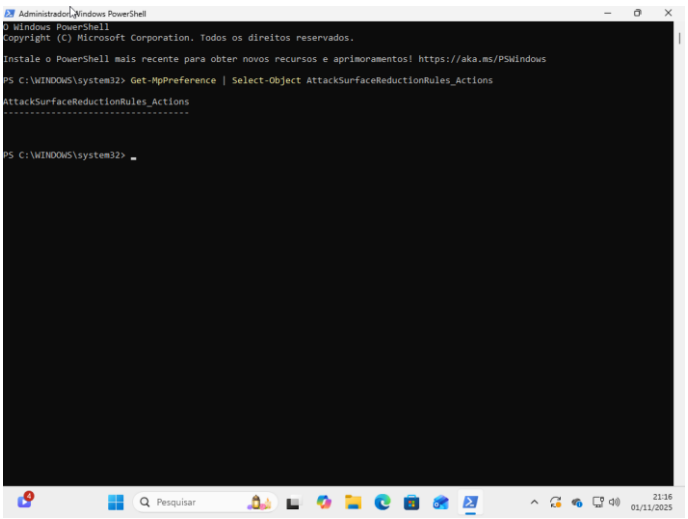
Figura 33 – Confirmação de execução como administrador



Fonte: Elaborado pelos autores (2025).

Dentro do PowerShell, foi executado o comando `Get-MpPreference | Select-Object AttackSurfaceReductionRules_Actions`. Esse comando retornou as configurações de preferências do Microsoft Defender, com a saída filtrada para exibir apenas o status das regras do ASR, representadas por suas GUIDs e respectivas ações. Cada GUID (identificador de regra) apresenta um status numérico: 0 para desativado, 1 para modo de auditoria e 2 para bloqueado. No entanto, como nenhuma regra estava configurada no ambiente, a saída do comando não apresentou GUIDs, indicando que não havia regras ativas, conforme ilustrada na Figura 34.

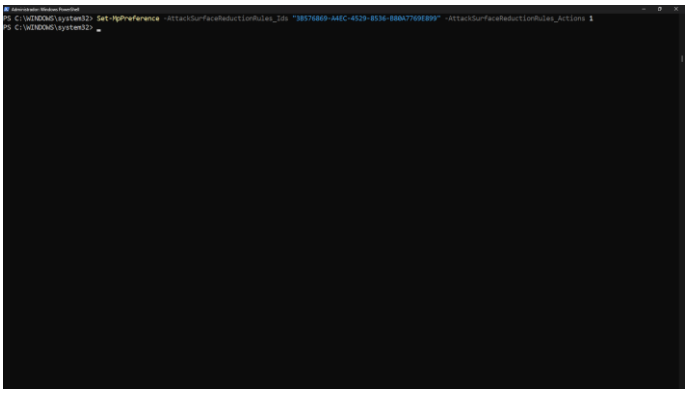
Figura 34 – Lista de regras ASR



Fonte: Elaborado pelos autores (2025).

Como evidenciado pela imagem, nenhuma regra estava configurada no momento. Para o experimento, foi aplicada uma regra que bloqueia a criação de conteúdo executável por aplicativos do Office, com o objetivo de impedir que documentos executem ou gerem arquivos executáveis, interrompendo, assim, a fase final de execução de *malwares* e *exploits*. Essa configuração foi realizada por meio do PowerShell, utilizando o comando `Set-MpPreference` para definir as preferências do Microsoft Defender, em conjunto com o parâmetro `-AttackSurfaceReductionRules_Ids` para especificar o GUID da regra e `-AttackSurfaceReductionRules_Actions 1` para ativá-la, conforme ilustrado na Figura 35.

Figura 35 – Criação da regra de bloqueio ASR



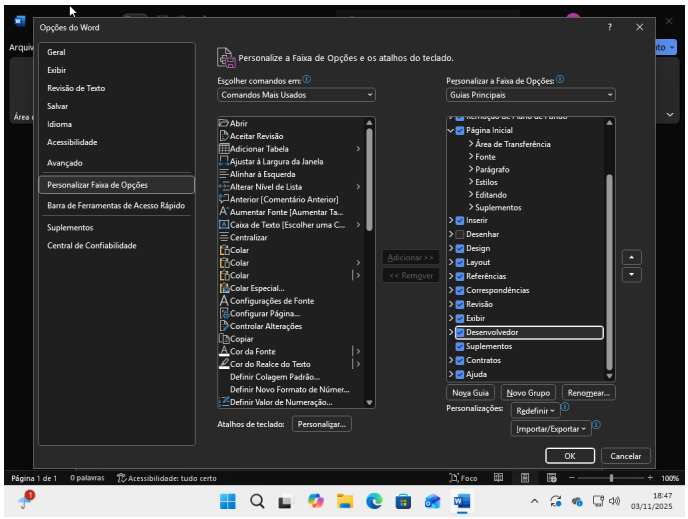
Fonte: Elaborado pelos autores (2025).

Cada regra do ASR aplica um tipo específico de proteção, incluindo o bloqueio de processos filhos iniciados pelo Office, a restrição de conteúdo executável embutido e a prevenção da execução de binários potencialmente maliciosos, entre outras. No experimento, foi utilizada a regra identificada pelo GUID 3B576869-A4EC-4529-8536-B80A7769E899, responsável por bloquear qualquer tentativa de criação de conteúdo executável por aplicativos do Office, representando de forma prática o objetivo do experimento proposto.

Dentro do Word foi criada uma macro simples que simulou a geração de um arquivo executável, de modo a evidenciar o bloqueio da criação do arquivo através da aplicação da regra ASR. Esse procedimento reproduziu a etapa final de um ataque, em que um documento do Office produz e tenta executar um binário, permitindo verificar se a regra de bloqueio impediria a conclusão da infecção.

Para implementar a macro foi habilitada a guia *Desenvolvedor*. No menu *Arquivo* logo após *Opções* e, em *Personalizar faixa de opções*, marcou-se a opção *Desenvolvedor* para então acessar o Editor do Visual Basic e inserir o script, conforme ilustrado na Figura 36.

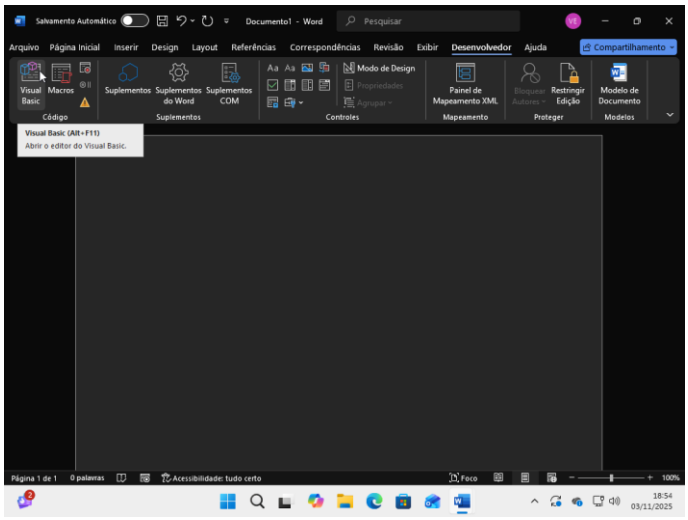
Figura 36 – Habilitar guia desenvolvedor no Word



Fonte: Elaborado pelos autores (2025).

Para acessar o Editor do Visual Basic criou-se um documento e selecionou-se a guia Desenvolvedor já habilitada, dentro dessa guia abriu-se a opção Visual Basic, conforme exemplificado na Figura 37.

Figura 37- Acesso ao Visual Basic no Word



Fonte: Elaborado pelos autores (2025).

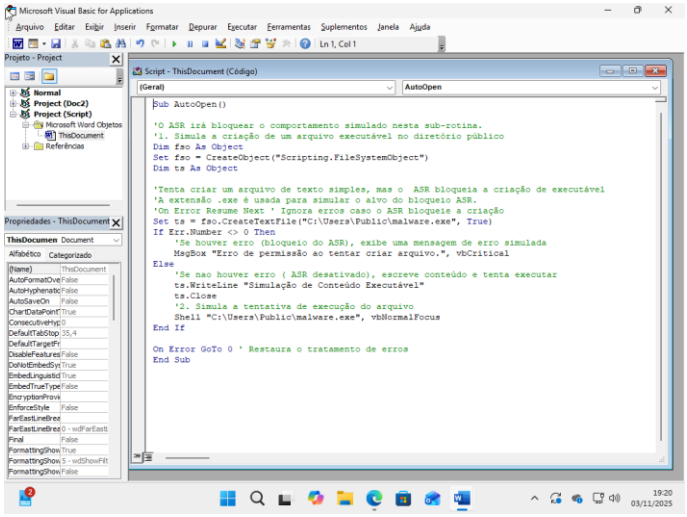
O código em *VBA* utilizado está descrito na Figura 38 e tem a finalidade exclusiva de simular o comportamento final de um ataque para testar a regra ASR. As principais instruções estão descritas abaixo:

`Sub AutoOpen()` definiu a subrotina que seria executada automaticamente ao abrir o documento, simulando execução involuntária de código por um usuário.

A chamada `CreateObject` com o objeto `Scripting.FileSystemObject` criou uma interface para manipulação de arquivos no sistema, técnica comumente utilizada por macros maliciosos para escrever arquivos no disco. A operação de criação de arquivo com `CreateTextFile` tentou gerar um arquivo executável em um diretório de acesso público, comportamento que representou o *payload* simulado e cujo bloqueio era o objetivo do teste.

Finalmente a invocação de Shell com o nome do arquivo e o parâmetro `vbNormalFocus` tentou executar o binário recém-criado, reproduzindo a etapa final de uma cadeia de infecção.

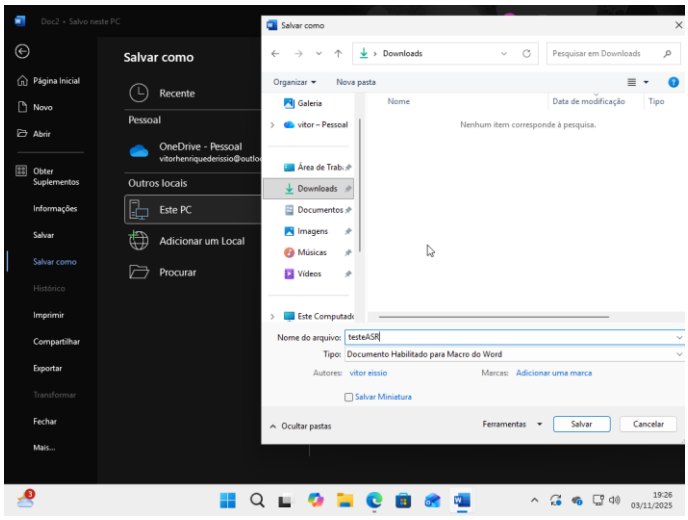
Figura 38 – Criação do script em Visual Basic



Fonte: Elaborado pelos autores (2025).

Após feito o *script*, o documento foi salvo com a extensão *.docm* da qual define como documento habilitado para macro do Word. O nome do arquivo será *testeASR*, conforme a Figura 39.

Figura 39 – Salvar documento habilitado para macro



Fonte: Elaborado pelos autores (2025).

2.4 Critérios de Avaliação e Métricas de Análise

Para garantir que os experimentos fossem analisados de forma objetiva, foram estabelecidos critérios de avaliação baseados no comportamento esperado de cada técnica, além de métricas que permitissem verificar sua eficácia dentro do cenário proposto. Para avaliar o método de detecção baseado em análise de dados, foram definidos critérios alinhados ao modelo de Bilge e Dumitraș (2012), que fundamenta a identificação de ataques de dia zero por meio da correlação entre dados de telemetria, reputação de arquivos e registros temporais. Nesse contexto, a principal métrica adotada consistiu em verificar se o arquivo malicioso utilizado no experimento apresentava sua primeira aparição em data anterior à divulgação da vulnerabilidade fictícia criada para o cenário, uma vez que essa relação temporal caracteriza a exploração de um ataque de dia zero. A avaliação considerou o registro de primeira ocorrência do arquivo na telemetria simulada, a reputação atribuída a esse arquivo conforme seu histórico de circulação no ambiente e a data de publicação do CVE fictício utilizado como referência para determinar o momento de divulgação da vulnerabilidade. O método foi considerado eficaz quando os dados indicaram coerência entre esses elementos, evidenciando que o arquivo apareceu antes da divulgação oficial da vulnerabilidade e, portanto, representava um evento típico de um ataque de dia zero dentro do modelo adotado. A repetição do experimento produziu resultados

consistentes, demonstrando que a técnica aplicada é reprodutível e adequada para o tipo de análise proposto.

No que se refere à técnica de prevenção, aplicada por meio do Windows Defender Exploit Guard com a Regra de Redução de Superfície de Ataque (ASR), a avaliação concentrou-se na capacidade do sistema de impedir a execução do comportamento malicioso simulado. A métrica adotada consistiu em verificar se a regra de Redução de Superfície de Ataque realmente bloqueou a ação e registrou o evento associado, evidenciando que o sistema reconheceu e interrompeu o comportamento suspeito. O método foi considerado eficaz quando a execução foi bloqueada e o registro correspondente confirmou a atuação da regra.

A aplicação desses critérios permitiu avaliar se as técnicas analisadas atendiam de fato ao objetivo da pesquisa, demonstrando, de forma clara e consistente, sua capacidade de detectar alterações e impedir comportamentos maliciosos dentro do ambiente controlado.

3 ANÁLISE DE RESULTADO

Não foram incluídos gráficos comparativos, pois o experimento trabalhou com apenas um único cenário de ataque, o que impediu de se utilizar qualquer gráfico devido à falta de um valor estatístico real. Como o objetivo do experimento foi apenas comprovar o funcionamento das técnicas empregadas e não avaliar desempenho em larga escala, a análise concentrou-se nos resultados obtidos a partir das técnicas empregadas. Dessa forma, os resultados consideram apenas o que foi observado durante a aplicação das técnicas, sem a necessidade de múltiplas amostras ou medições repetidas.

Os testes foram realizados em um ambiente controlado, seguindo exatamente as etapas descritas na metodologia, para que fosse possível avaliar, com clareza, como as técnicas selecionadas se comportariam diante de uma situação de risco. A proposta visou simular os procedimentos utilizados para detectar ou bloquear uma ameaça ainda desconhecida.

Para tornar esse processo mais completo, foram utilizados dois sistemas operacionais diferentes Linux e Windows 11, permitindo observar como as soluções se adaptam a contextos distintos de uso. A análise dos resultados foi dividida em duas partes: primeiro, a aplicação do método de detecção baseado em análise de dados, e depois a aplicação das regras de prevenção com o Windows Defender Exploit Guard. Em cada etapa, foram registrados os comandos utilizados, as evidências visuais e as conclusões tiradas a partir do que foi observado, de modo que todo o experimento pudesse ser compreendido e replicável com facilidade.

3.1 Resultado do método de detecção

Nesta subseção, é apresentada a aplicação prática da técnica de detecção baseada em análise de dados, proposta por Bilge e Dumitras (2012). O objetivo deste experimento é demonstrar o processo de identificação de ataques de dia zero por meio da coleta, correlação e análise de informações sobre vulnerabilidades e ameaças registradas em bases de dados especializadas. O método consiste em relacionar vulnerabilidades conhecidas, identificadas por seus respectivos CVE, aos malwares que as exploram, utilizando dados de telemetria e reputação de arquivos obtidos de

ferramentas de segurança. Essa abordagem permite reconhecer comportamentos maliciosos e identificar possíveis ataques de dia zero antes mesmo da divulgação pública das vulnerabilidades. A seguir, são descritas as etapas do procedimento, acompanhadas de representações gráficas e evidências coletadas durante a simulação, a fim de demonstrar a aplicabilidade e a eficácia da técnica de detecção proposta.

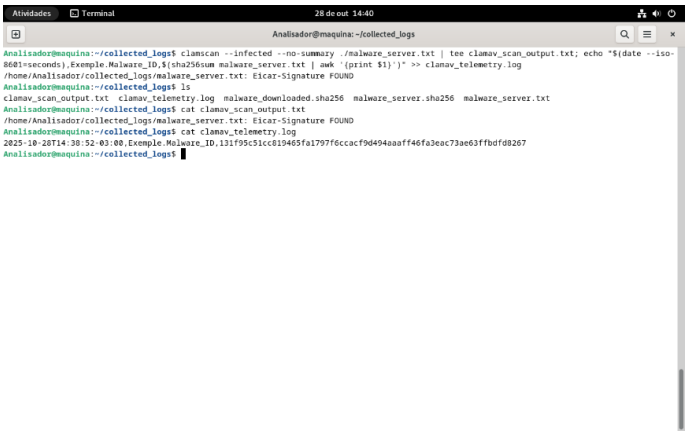
O processo de análise e decisão de ataque de dia zero ocorreu na máquina Analisador e foi a etapa final do laboratório, onde os dados coletados foram processados para determinar se a infecção da máquina Vítima se enquadra em um cenário de *zero-day*.

Para o processo de telemetria, o objetivo foi simular a detecção do arquivo de teste pelo antivírus e registrar o evento como telemetria, para isso, foi executado o `clamscan --infected --no-summary ./malware_server.txt`, este comando utilizou o ClamAV para escanear a cópia do arquivo `malware_server.txt`, as opções `--infected` e `--no-summary` garantiram que apenas os arquivos detectados como infectados fossem listados, sem o resumo final.

Na sequência foi executado o comando `tee clamav_scan_output.txt` que produziu o redirecionamento da saída do comando para a tela e, ao mesmo tempo, salvou no arquivo `clamav_scan_output.txt`, garantindo o registro da detecção.

Por último, ocorreu a criação de uma linha de *log* simulando a telemetria, que continha o *timestamp* atual, um virus ID fictício chamado `Exemple.Malware_ID` e o *hash* SHA256 do arquivo que foi anexada ao log de telemetria do ClamAV. A expressão final utilizada para esse processo foi `echo "$(date --iso-8601=seconds), Example.MALWARE_ID, $(sha256sum malware_server.txt | awk '{print $1}')" >> clamav_telemetry.log`, conforme representado pela figura 40.

Figura 40 – Simulação do processo de telemetria



Fonte: Elaborado pelos autores (2025).

O resultado desse processo foi o registro de um evento de detecção salvo no arquivo `clamav_telemetry.log`, que serviu como base de dados para o analisador identificar o momento em que o antivírus, simulado pelo ClamAV, passou a reconhecer o arquivo como malicioso, exemplificando o funcionamento da telemetria.

A próxima etapa, é a simulação da reputação binária, da qual simula a coleta de logs de *downloads* para determinar qual foi o momento que o arquivo malicioso foi visto pela primeira vez na rede do laboratório.

Na etapa seguinte ocorreu a simulação da reputação binária, que reproduziu a coleta de registros de download para determinar o instante em que o arquivo malicioso foi visto pela primeira vez na rede do laboratório. O comando `grep 'GET /malware.txt'` pesquisou no log do servidor HTTP todas as ocorrências de requisições ao arquivo `malware.txt`. Como o servidor registrava cada solicitação recebida, esse filtro permitiu isolar apenas as linhas correspondentes aos downloads do arquivo. O comando seguinte `head -n1 > first_seen.log` faz com que apenas a primeira dessas linhas seja mantida, ou seja, o primeiro download registrado, essa linha é então gravada no arquivo `first_seen.log`.

Logo em seguida, o comando `echo "first_seen_timestamp: $(head -n1 first_seen.log)" > reputation_record.txt` leu o conteúdo da primeira linha de `first_seen.log` e o inseriu dentro de uma nova linha de texto que começou com o título `first_seen_timestamp`. Essa linha é gravada em um novo arquivo chamado `reputation_record.txt`, que representou o registro de reputação

daquele binário, ou seja, a sua identificação através do *hash* com o momento em que ele foi visto pela primeira vez.

Por fim, o comando `cat malware_server.sha256 >> reputation_record.txt` acrescenta ao arquivo `reputation_record.txt` o conteúdo de `malware_server.sha256`, que contém o *hash* SHA256 do arquivo hospedado no servidor. Dessa forma, o arquivo final `reputation_record.txt` passou a conter duas informações de log: a ocorrência do primeiro *download* do arquivo e o seu *hash*. Etapa ilustrada na Figura 41.

Figura 41– Simulação do processo de reputação binária

Fonte: Elaborado pelos autores (2025).

A última etapa consistiu na criação de um CVE fictício com data de publicação posterior à data da primeira ocorrência registrada, de modo a simular um cenário de ataque de dia zero. Esse procedimento teve caráter demonstrativo, pois em ambientes reais utiliza se um CVE oficial com data verídica.

Para a simulação foi definido o CVE com publicação em 2025/10/29 22:00:00 e o identificador 2025_12345. Foram criados dois arquivos temporários: CVE_ID contendo o identificador da vulnerabilidade e T_CVE contendo a data de publicação. Em seguida esses dois valores foram gravados no arquivo `cve_disclosure_date.txt`, conforme exemplificado na Figura 42.

Figura 42– Criação do CVE fictício

Fonte: Elaborado pelos autores (2025).

A decisão foi tomada ao comparar os *hashes* dos arquivos e posteriormente comparar com a telemetria e com a reputação binária. O utilitário diff foi utilizado para comparar os dois arquivos de *hashes:* o arquivo `malware_server.sha256` corresponde ao hash do arquivo original do servidor, enquanto `malware_downloaded.sha256` corresponde ao *hash* do arquivo baixado do servidor pela VM vítima. Desse modo o analisador conseguiu confirmar que o arquivo baixado pela vítima era o mesmo hospedado no servidor e o mesmo detectado pelo antivírus e registrado na reputação binária, conforme a figura 43.

Figura 43 – Comparação dos arquivos para confirmar integridade

Fonte: Elaborado pelos autores (2025).

Em seguida, comparou-se o instante de exposição da vítima com a data de divulgação pública da vulnerabilidade simulada pelo CVE para determinar se a exposição configurava um ataque de dia zero. O Quadro 3 demonstra essa relação.

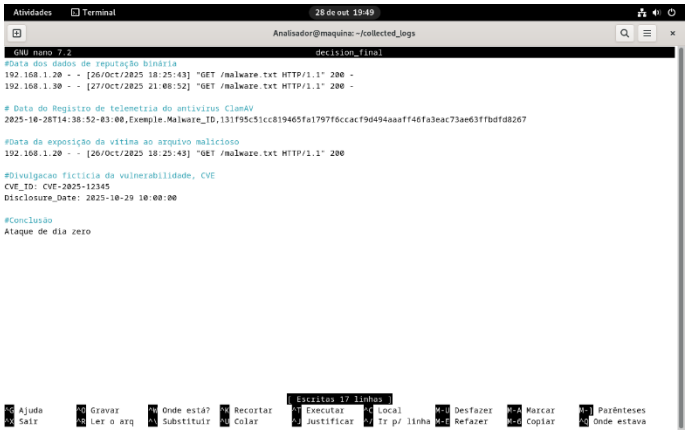
Quadro 4 – Processo de decisão de dia zero

Cenário	Condição	Conclusão
Ataque de dia zero	Tempo_Vítima < Tempo_CVE	O arquivo foi baixado e a vítima foi exposta antes da divulgação pública da vulnerabilidade
Não é ataque de dia zero	Tempo_Vítima ≥ Tempo_CVE	A exposição ocorreu após a vulnerabilidade se tornar pública

Fonte: Elaborado pelos autores (2025).

Portanto, de acordo com o experimento prático realizado, confirmou-se que o *malware* simulado caracterizou um ataque de dia zero, pois a máquina vítima realizou o *download* do arquivo malicioso em 26 de outubro, a telemetria do antivírus registrou sua detecção em 28 de outubro e a divulgação pública da vulnerabilidade, representada pelo CVE correspondente, ocorreu posteriormente em 29 de outubro, configurando assim um ataque de dia zero, a organização dos dados foi ilustrada na Figura 44.

Figura 44– Conclusão da lógica do ataque de dia zero



Fonte: Elaborado pelos autores (2025).

Como etapa final, de acordo com o método de Bilge e Dumitras (2012), os resultados obtidos no experimento foram exemplificados em uma tabela final, conforme a Tabela 1, contendo as informações cruciais do experimento.

Tabela 1 - Classificação dos resultados do método de detecção

Vulnerabilidade dia zero	Assinatura de antivírus	Data de Divulgação	Divulgação pública do exploit	Início de Ataque	Variantes	Máquinas Alvo
CVE-2025-12345	Exemple.Malware_ID	2025-10-29	Desconhecido	2025-10-26	1	1

Fonte: Adaptado de Bilge e Dumitraș (2012).

Dessa forma, o método de detecção baseado em análise de dados demonstrou resultados coerentes com o modelo proposto por Bilge e Dumitras (2012), confirmando sua eficácia na identificação de ataques de dia zero a partir do cruzamento de dados de divulgação de vulnerabilidades conhecidas com registros de reputação binária de arquivos maliciosos. Por meio da comparação entre as datas de detecção e as de divulgação das vulnerabilidades, foi possível observar que determinadas falhas foram exploradas antes de sua publicação oficial, caracterizando o comportamento típico de um ataque de dia zero.

Os resultados obtidos mostraram-se compatíveis, relativo ao laboratório simulado, com os apresentados pelos autores, evidenciando que o método foi tecnicamente viável, reprodutível e aplicável em estudos de segurança da informação. Além disso, o cruzamento de dados entre registros de telemetria antivírus e informações de reputação binária mostrou-se uma estratégia eficaz para identificar possíveis explorações antes da divulgação pública das falhas, contribuindo para aprimorar os processos de monitoramento e a priorização de correções de segurança em sistemas afetados, bem como para incentivar a implementação de um gerenciamento contínuo de vulnerabilidades e a aplicação de patches sempre que disponíveis.

3.2 Resultado do método de prevenção

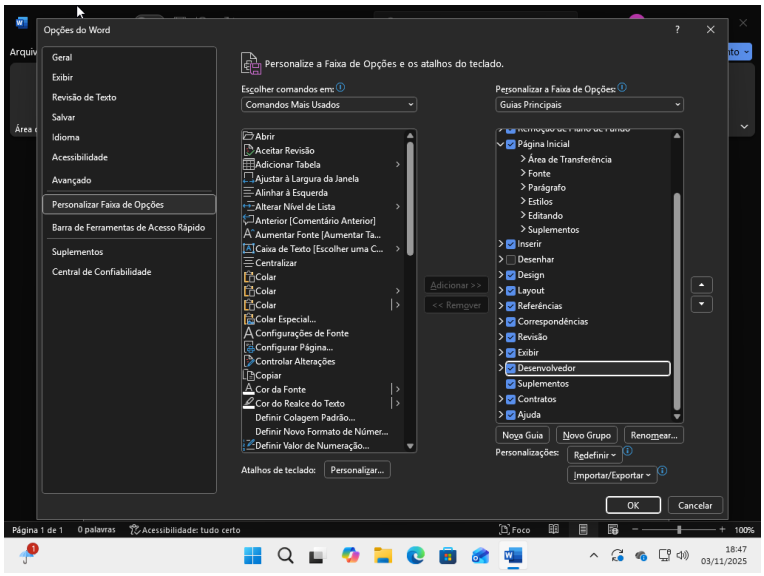
Nesta etapa foram apresentados os resultados da aplicação prática da técnica de prevenção de ataques de dia zero empregando o Windows Defender Exploit Guard (WDEG), recurso nativo do Windows 11. O experimento teve por objetivo demonstrar o funcionamento da regra de Redução da Superfície de Ataque (ASR), componente responsável por monitorar e bloquear comportamentos suspeitos que possam indicar execução de código malicioso ou exploração de vulnerabilidades desconhecidas. Entre as ações observadas durante os testes estavam a criação de arquivos executáveis, o

uso de macros potencialmente perigosas e a execução de *scripts* em documentos do Microsoft Office, vetores frequentemente explorados em ataques de dia zero.

A escolha do WDEG justificou se por se tratar de uma solução preventiva integrada ao sistema operacional, que combina políticas automatizadas com proteção em tempo real, dispensando a necessidade de *softwares* complementares para as defesas básicas. Essa característica mostrou se relevante em cenários corporativos, onde a detecção e o bloqueio rápidos de comportamentos maliciosos ajudam a conter a propagação de ameaças e a reduzir impactos operacionais.

O experimento foi executado em ambiente controlado e consistiu na simulação de um *script* malicioso inserido em um documento do Word do pacote Office 365. Convém observar que o suporte nativo do ASR aos aplicativos do Office foi introduzido a partir das versões de 2021, razão pela qual se utilizou o Office 365 no laboratório como explicado anteriormente. Durante o teste foi verificado que a regra ASR bloqueou automaticamente a tentativa de criação do arquivo executável e registrou o evento nos logs de segurança do sistema. Os resultados a seguir incluem a sequência de procedimentos realizados, os comandos empregados e as evidências coletadas que comprovam a eficácia e a aplicabilidade do recurso na prevenção de ameaças de dia zero. Para a implementação do macro foi habilitada a guia *Desenvolvedor* no Word por meio de *Opções*, em *Personalizar faixa de opções*, esta opção habilita o Editor do Visual Basic para inserir o *script*, conforme ilustrado na Figura 45.

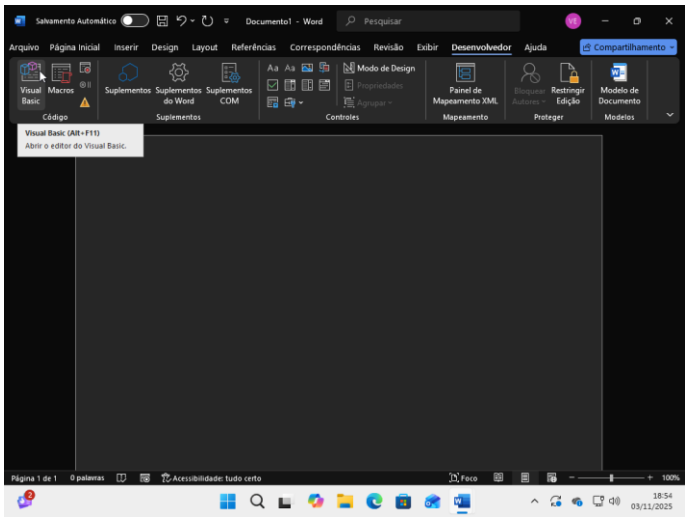
Figura 45 – Habilitar guia desenvolvedor no Word



Fonte: Elaborado pelos autores (2025).

Para acessar o Visual Basic, criou-se um documento e selecionou-se a guia *Desenvolvedor*, previamente habilitada. Dentro dessa guia, escolheu-se a opção *Visual Basic* para abrir o editor utilizado na criação do *script*, conforme exemplificado na Figura 46.

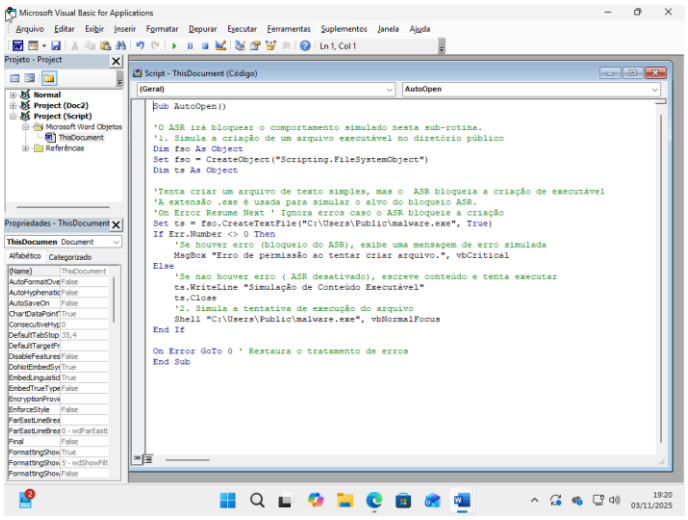
Figura 46- Acesso ao Visual Basic no Word



Fonte: Elaborado pelos autores (2025).

O código em VBA utilizado está descrito na Figura 47. Na sequência estão as instruções principais e sua função no teste. `Sub AutoOpen()` definiu a sub-rotina executada automaticamente ao abrir o documento, simulando execução involuntária de código. `CreateObject("Scripting.FileSystemObject")` criou um objeto para manipulação de arquivos, técnica comumente empregada por macros maliciosas.

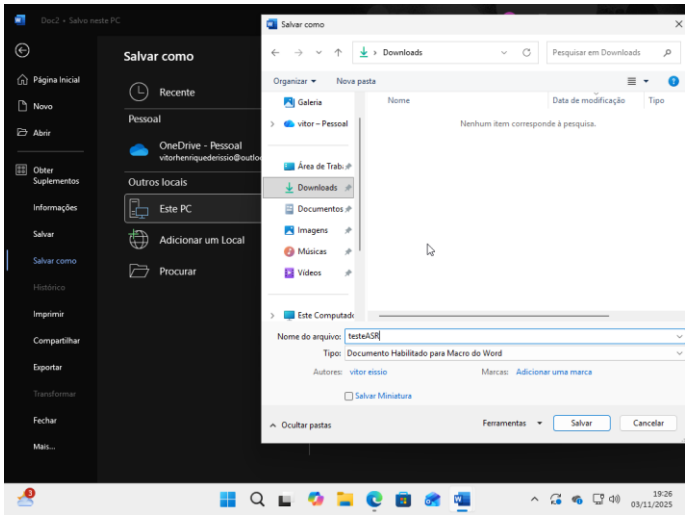
Figura 47 – Criação do script em Visual Basic



Fonte: Elaborado pelos autores (2025).

A chamada `fso.CreateTextFile("C:\Users\Public\malware_sim.exe", True)` tentou gerar um arquivo executável em um local de acesso público, comportamento crítico que a regra ASR deveria bloquear. Por fim, `Shell "C:\Users\Public\malware_sim.exe", vbNormalFocus` tentou executar o binário recém-criado. Após feito o *script*, o documento será salvo com a extensão .docm da qual define como documento habilitado para macro do Word, o nome do arquivo será `testeASR`, conforme a Figura 48.

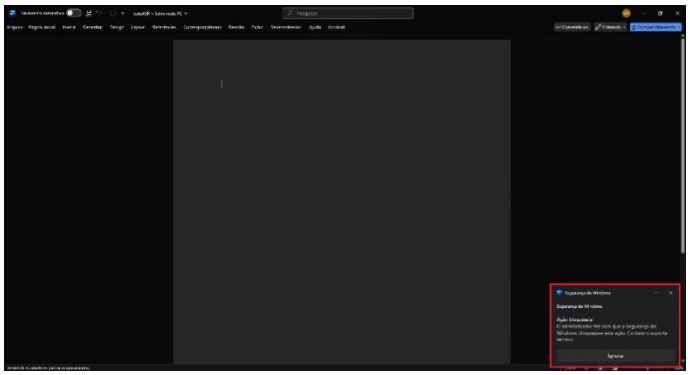
Figura 48 – Salvar documento habilitado para macro



Fonte: Elaborado pelos autores (2025).

Após a implementação do *script* o documento foi salvo com a extensão *.docm* que identifica documentos do Word habilitados para macro. O arquivo recebeu o nome `testeASR` conforme ilustrado na Figura 49.

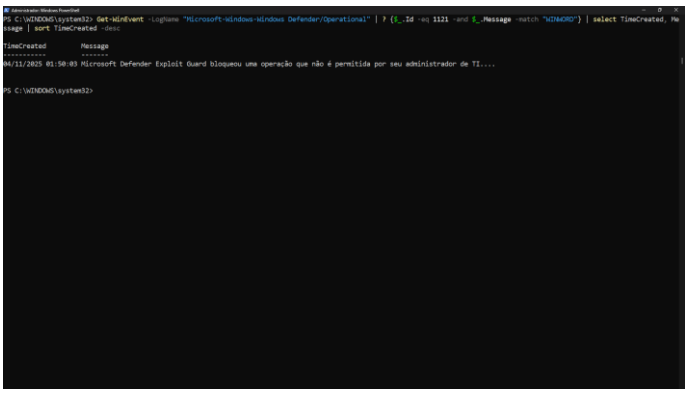
Figura 49 – Alerta do Windows do bloqueio feito pela regra ASR



Fonte: Elaborado pelos autores (2025).

A etapa final para verificar o sucesso do bloqueio realizado pela regra implementada consistiu na análise dos registros de *log* gerados pelo sistema, conforme previsto no fluxo do processo. Essa verificação foi feita no PowerShell por meio do comando: `Get-WinEvent -LogName "Microsoft-Windows-Windows Defender/Operational" | ? {$_.Id -eq 1121 -and $_.Message -match "WINWORD"} | select TimeCreated, Message | sort TimeCreated -desc`. Esse comando exibiu na tela os registros gravados pelo sistema, mostrando o evento correspondente ao bloqueio do *script*, o que comprovou o funcionamento da regra ASR como parte da etapa final do processo, conforme a figura 50.

Figura 50 – Registro log do bloqueio do script



Fonte: Elaborado pelos autores (2025).

Dessa forma, o método de prevenção utilizando o recurso Attack Surface Reduction (ASR), integrante do Windows Defender Exploit Guard (WDEG), demonstrou resultados consistentes e alinhados aos objetivos propostos neste trabalho. O experimento, conduzido exclusivamente com o Microsoft Word, comprovou a capacidade da ferramenta em bloquear automaticamente comportamentos suspeitos, como a tentativa de criação de arquivos executáveis a partir de macros, vetor frequentemente explorado em ataques de dia zero.

Os resultados obtidos corresponderam às observações de Kutsovsky (2017), que destaca a eficácia do ASR na detecção e bloqueio de atividades maliciosas em aplicativos do Office, mitigando ameaças que exploram vulnerabilidades ainda desconhecidas. Durante o teste, o bloqueio ocorreu em tempo real e foi devidamente registrado nos *logs* do sistema, confirmando o funcionamento correto da regra configurada e a integração eficiente com o Windows Defender.

Diferentemente dos antivírus tradicionais baseados em assinaturas, o ASR atua de forma comportamental e preventiva, identificando ações potencialmente perigosas antes que possam comprometer o sistema. Essa característica reforçou sua relevância e eficiência como mecanismo nativo de defesa do Windows, especialmente em ambientes corporativos que demandam proteção ativa contra ameaças emergentes.

Ainda segundo Kutsovsky (2017), para qualquer aplicação de negócios em uso em uma organização, é possível definir exclusões baseadas em arquivos e pastas. Além disso, o ASR permite que administradores apliquem políticas específicas para clientes de *e-mail* em dispositivos corporativos, ampliando a capacidade de controle sobre o ambiente.

Portanto, a técnica de prevenção mostrou-se eficaz no bloqueio de comportamentos suspeitos, confirmando o recurso ASR do Windows Defender Exploit Guard como uma solução confiável, acessível e aplicável na proteção contra-ataques de dia zero em sistemas Windows.

3.3 Comparação entre os métodos aplicados

A comparação entre os métodos aplicados neste estudo evidencia que cada técnica atua em momentos distintos do ciclo de ataque e oferece contribuições complementares para a segurança do sistema. O método de detecção baseado em análise de dados tem característica analítica e retrospectiva, focado na identificação de

evidências que indiquem possível exploração antes da divulgação oficial de uma vulnerabilidade. Ele se apoia em dados como linha do tempo de ocorrência, reputação de arquivos e registros de atividade, permitindo reconhecer comportamentos suspeitos mesmo quando o *malware* ainda não é amplamente conhecido. Dessa forma, sua principal função é fornecer visibilidade, reconstruir eventos e permitir a compreensão se um ataque de dia zero possivelmente ocorreu.

Por outro lado, o método de prevenção utilizando o Windows Defender Exploit Guard com a regra ASR apresenta uma característica proativa e imediata. Em vez de analisar histórico ou reputação, sua ação ocorre no momento da execução: qualquer comportamento considerado potencialmente malicioso é bloqueado antes de causar impacto no sistema. Enquanto o método de detecção compara dados, o método de prevenção impede que o comportamento seja concluído, interrompendo a cadeia de ataque já na fase inicial, especialmente em situações que envolvem macros, scripts ou tentativas de criação de executáveis.

Essa diferença fundamental demonstra que os métodos não competem entre si, mas se complementam. A detecção fornece conhecimento, rastreabilidade e entendimento sobre o evento, enquanto a prevenção reduz a superfície de ataque e impede que ações suspeitas sejam concluídas. A partir dos resultados obtidos, fica evidente que uma estratégia de segurança eficaz depende da combinação de mecanismos capazes tanto de detectar quanto de bloquear atividades maliciosas, reforçando a importância de abordagens integradas quando se trata de ameaças avançadas como ataques de dia zero.

3.4 Limitação e Discussão Crítica

Apesar dos resultados apresentados, este trabalho possui limitações importantes que devem ser reconhecidas para uma interpretação adequada das conclusões e para possibilitar investigações futuras. Em primeiro lugar, o uso do ClamAV como ferramenta de análise no ambiente Linux impõe restrições técnicas, pois se trata de um antivírus de código aberto cuja base de assinaturas é menos abrangente que soluções comerciais de mercado e não foi concebida para detecção proativa de ameaças avançadas. Logo, a ausência de detecções pelo ClamAV não pode ser interpretada como garantia de segurança, assim como suas detecções não representam, por si só, desempenho comparável ao de EDRs comerciais. Portanto, os resultados dependem

do escopo funcional dessa ferramenta e não representam a universalidade do comportamento de soluções de detecção no mundo real.

Em segundo lugar, a simulação de arquivos maliciosos neste estudo, incluindo o uso de arquivos de teste e cenários controlados, não reproduz integralmente a complexidade e a criatividade de malware real em ambiente de produção. O arquivo EICAR e artefatos similares foram empregados apenas para fins de validação funcional; contudo, esses arquivos não incorporam técnicas de ofuscação, evasão ou persistência observadas em ameaças reais. Assim, a resposta observada nas ferramentas e regras configuradas pode divergir do comportamento perante amostras reais encontradas em ataques de dia zero reais.

Outra limitação relevante refere-se à dependência de telemetria e de dados de reputação para a metodologia de detecção adotada. A técnica inspirada em Bilge e Dumitraș (2012) pressupõe a disponibilidade de registros temporais confiáveis e de histórico de circulação dos arquivos, em ambientes sem telemetria consolidada ou com baixa visibilidade, a eficácia dessa abordagem tende a reduzir-se significativamente. Da mesma forma, a criação e utilização de um CVE fictício para fins experimentais representa um componente metodológico necessário, porém simplificador, que não replica o processo de divulgação, análise e correção que envolve vulnerabilidades reais.

Quanto à prevenção por meio do Windows Defender Exploit Guard e das regras ASR, existem limitações operacionais que se destacam. As regras ASR podem gerar falsos positivos, dependendo das políticas e do perfil de uso do usuário, impactando a experiência e possivelmente levando a bloqueios indevidos de aplicações legítimas. Além disso, a eficácia do ASR depende fortemente da correta configuração e de políticas complementares do Defender, em contexto corporativo, sua operação ideal requer integração com políticas de grupo, registro central de eventos e procedimentos de exceção, fatores que não foram integralmente reproduzidos no laboratório controlado deste estudo. Assim, embora o bloqueio observado demonstre capacidade de mitigação, a generalização desses resultados deve considerar a variabilidade de configuração e o risco de bloqueios excessivos em ambientes produtivos.

Também é importante salientar limitações relativas ao escopo experimental: o estudo foi conduzido em máquinas virtuais e em cenários isolados (Linux para detecção e Windows para prevenção), o que facilita reprodução, mas reduz o realismo em comparação a infraestruturas mais complexas e interconectadas. O experimento e a quantidade de ataques testados foram reduzidos de propósito para tornar o projeto

viável, o que significa que não é possível tirar conclusões fortes sobre taxas reais de detecção, falsos positivos ou falsos negativos em um cenário maior. Por fim, o experimento não simulou um ataque de *zero-day* em sentido literal, isto é, não envolveu a criação e exploração de uma vulnerabilidade inédita no *software* alvo, o que reforça a necessidade de interpretar os resultados como prova de conceito e recorte experimental, não como avaliação de desempenho operacional das ferramentas.

Para reduzir essas limitações em trabalhos futuros, recomenda-se complementar o experimento com antivírus comerciais para comparação direta, ampliar a variedade e complexidade das amostras, integrar conjuntos de telemetria mais representativos e testar as regras ASR em políticas de grupo e em ambientes corporativos com procedimentos de exceção. Estudos posteriores também poderiam empregar SIEM para correlação em larga escala, *sandboxing* dinâmico para análise comportamental aprofundada e ensaios controlados que gerem *exploits* mais próximos de *zero-days* reais, respeitando considerações éticas e legais. Essas medidas tornariam os resultados mais confiáveis e permitiriam analisar melhor a precisão das detecções e a ocorrência de falsos positivos e falsos negativos.

Em suma, este trabalho configura-se como um recorte prático e controlado das possibilidades de defesa em relação a ataques de dia zero, oferecendo contribuições para compreensão e demonstração de conceitos. Ao mesmo tempo, é indispensável evitar generalização indevidas para ambientes e ameaças mais complexos.

CONSIDERAÇÕES FINAIS

Os resultados obtidos demonstraram que o trabalho atendeu aos objetivos gerais e específicos propostos, permitindo analisar de forma prática e conceitual técnicas de detecção e prevenção de ataques de dia zero. A partir dos objetivos específicos, foi possível estruturar uma pesquisa sólida que abordou amplamente tanto teoria quanto aplicação prática, demonstrando, de forma integrada, como diferentes métodos podem ser combinados para aumentar o nível de segurança dos sistemas.

A revisão conceitual inicial permitiu compreender os fundamentos da informação, da segurança da informação e dos conceitos essenciais, estabelecendo a base teórica necessária para o desenvolvimento da pesquisa. A análise das vulnerabilidades e ameaças digitais possibilitou entender como falhas se transformam em ataques, enquanto a abordagem das consequências jurídicas reforçou a importância da conformidade e da responsabilidade organizacional contra os ataques cibernéticos. O estudo do caso real MOVEit SQLi contribuiu para contextualizar a gravidade e a complexidade dos ataques de dia zero em ambientes corporativos.

Com base nesse embasamento teórico, foram estudadas diversas técnicas de detecção e prevenção, das quais duas foram selecionadas para aplicação prática. O método de detecção baseado em análise de dados demonstrou ser eficaz na identificação de possíveis ameaças de dia zero, permitindo reconhecer arquivos desconhecidos e não catalogados por assinaturas de antivírus no momento da exploração, validando a proposta de detecção de ameaças que exploram as vulnerabilidades não divulgadas. O método de prevenção, implementado por meio do Windows Defender Exploit Guard, mostrou-se eficiente na contenção das ações executadas por scripts desconhecidos, bloqueando a execução e registrando o evento. A execução dos experimentos em ambiente controlado permitiu avaliar o desempenho e resultados das técnicas, confirmando a hipótese de que a operação em conjunto entre detecção e prevenção é essencial para a mitigação de ataques de dia zero.

Como sugestão de melhoria, observou-se que o método de detecção pode ser aprimorado para aplicação em ambientes com grandes volumes de dados. Nesse sentido, sugere-se a implementação de um banco de dados específico para o tratamento e relação das informações coletadas, de forma a ampliar a capacidade e otimizar a identificação de ameaças. Essa proposta indica o SQLite, citado

anteriormente no trabalho apenas para exemplificar o uso em contextos reais de manipulação de grandes conjuntos de dados, que poderia ser utilizado como base para aprimorar a eficiência do método. Além disso, a automatização de processos utilizando programação, especificamente a linguagem Python, que oferece bibliotecas para automatização de tarefas como mencionado no laboratório, seria essencial para tornar todo o processo mais eficiente e otimizado, considerando grandes volumes de dados.

Quanto ao método de prevenção, uma melhoria proposta consiste em adicionar mais regras diversificadas no componente ASR do Windows Defender Exploit Guard, abrangendo não apenas scripts em Visual Basic, mas também ações relacionadas ao Microsoft Office, além de acesso a pastas e anexos de e-mails. Uma melhoria sugerida também é o uso em conjunto dessas regras com políticas aplicadas a clientes de e-mail, ampliando o alcance da defesa e fortalecendo a proteção contra ameaças adicionais de ataques.

As demais técnicas de detecção e prevenção abordadas ao longo deste trabalho também se mostraram relevantes e podem ser utilizadas como objeto de estudo em futuras pesquisas ou como base para o desenvolvimento ampliado do presente trabalho, permitindo novas abordagens com o uso de tecnologias complementares, como *machine learning* e análise comportamental avançada.

Por fim, conclui-se que soluções em conjunto de detecção e prevenção representam o método mais eficiente para o fortalecimento da segurança da informação, evidenciando a importância de estratégias de segurança bem estruturadas e constantemente aprimoradas diante do cenário crescente de ameaças digitais.

Como continuidade do presente trabalho, recomenda-se a utilização de soluções corporativas completas, como antivírus de nova geração e sistemas de monitoramento e gestão de eventos de segurança (SIEM), possibilitando a correlação em larga escala de indicadores de comprometimento (IOC) e indicadores de ataque (IOA). Outro avanço natural seria a inclusão de ambientes controlados de análise automática de malware, conhecidos como *sandboxing*, com execução dinâmica real, além da simulação de cenários de invasão próximos ao contexto de um ataque verdadeiro, permitindo avaliar comportamento, técnicas de evasão, falsos positivos e falsos negativos em condições mais próximas de ambientes reais. Tais amplificações tornariam os resultados mais robustos, comparáveis ao estado atual da prática no setor e alinhados às exigências reais de defesa cibernética de organizações.

REFERÊNCIAS

ANDRADE, Sara. **A informação na sociedade contemporânea: uma breve abordagem sobre a sociedade da informação, o fenômeno global e a mundialização da cultura**. Revista UNI-RN, Natal, v. 1, n. 1, p. 207, 2001. Disponível em: https://revistas.unirn.edu.br/index.php/revistaunirn/article/view/34. Acesso em: 27 maio 2025.

BASTOS, Athena. **Quais são os pilares e as funções da segurança da informação?** Alura, [S.l.], 2023. Disponível em: https://www.alura.com.br/empresas/artigos/seguranca-da-informacao. Acesso em: 6 out. 2025.

BILGE, Leyla; DUMITRAS, Tudor. **Before we knew it: an empirical study of zero-day attacks in the real world**. Proceedings of the 2012 ACM Conference on Computer and Communications Security, Raleigh, v. 2012, p. 833-844, 2012. Disponível em: https://www.researchgate.net/publication/262240606_Before_we_knew_it_An_empirical_study_of_zero-day_attacks_in_the_real_world. Acesso em: 27 maio 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 (Marco Civil da Internet). Jusbrasil, [S.l.], 2018. Disponível em: https://www.jusbrasil.com.br/legislacao/612902269/lei-13709-18. Acesso em: 6 out. 2025.

BRAZ, G. V. C. **Segurança na era da IoT: prevenção de vulnerabilidades no ciclo de vida do software**. 2023. 107 f. Trabalho de Conclusão de Curso (Bacharelado em Engenharia de Software) – Universidade de Brasília, Faculdade UnB Gama, Brasília, 2023. Disponível em: https://bdm.unb.br/bitstream/10483/39146/1/2023_GuilhermeVerissimoCerveiraBraz_tcc.pdf. Acesso em: 11 out. 2025.

BUCKBEE, Michael. **Zero-Day Vulnerability Explained**. Varonis, 16 jun. 2023. Disponível em: https://www.varonis.com/blog/zero-day-vulnerability. Acesso em: 27 maio 2025.

BUCKLAND, Michael K. **Informação como coisa**. Journal of the American Society for Information Science (JASIS), [S.l.], v. 45, n. 5, p. 351-360, 1991. Tradução livre de Luciane Artêncio. Disponível em: < <https://www.cin.ufpe.br/~cjgf/TECNOLOGIA%20-%20material%20NAO-CLASSIFICADO/Informacao%20como%20Coisa%20%28thing%29.pdf>. Acesso em: 6 out. 2025.

CAMARGO, Pamela Sena. **A importância da informação: como instrumento de apoio à gestão**. 2017. 38 f. Trabalho de Conclusão de Curso (Graduação em Sistemas da Informação) - Anhanguera Educacional, São Paulo, 2017. Disponível em: <https://repositorio.pgsscogna.com.br/bitstream/123456789/27178/1/TCC2_3-definitivo--+PDF.pdf>. Acesso em: 6 out. 2025.

CARANTI, Larissa Monaco; FUKUHARA, Tatiana Lie. **Responsabilização de empresas à luz da Lei Geral de Proteção de Dados**. Revista de Direito Internacional e Globalização Econômica, São Paulo, v. 8, n. 8, 2021. Disponível em: <https://revistas.pucsp.br/index.php/DIGE/article/view/56260>. Acesso em: 6 out. 2025.

CARMO, U. A.; SIQUEIRA, I. P.; MARINHO, M. H. N.; RISSI, G. F.; TOMASIN, S. G. **Análise de vulnerabilidade em concentradores de dados de infraestrutura AMI**. Principia: Revista do Instituto Federal da Paraíba, João Pessoa, v. 1, n. 55, p. 213-224, 2021. Disponível em: https://periodicos.ifpb.edu.br/index.php/principia/article/viewFile/4764/1728. Acesso em: 6 out. 2025.

CARVALHO, Ana Caroline Santana de. **A importância das redes sociais para o empreendedorismo: a visão de empreendedores digitais e alunos de administração de uma instituição de ensino superior**. 2024. 21 f. Trabalho de Conclusão de Curso (Graduação em Administração) - Universidade Federal do Amazonas, Manaus, 2024. Disponível em: <https://riu.ufam.edu.br/bitstream/prefix/7985/5/TCC_AnaCarolineCarvalho.pdf>. Acesso em: 6 out. 2025.

CESARANO, Carmine. **Security assessment and hardening of fog computing systems**. 2023. Disponível em: https://arxiv.org/pdf/2308.12707. Acesso em: 11 jun. 2025.

CHARRIER, C.; SADOWSKI, J.; LECIGNE, C.; STOLYAROV, V. **Hello 0-days, my old friend: a 2024 zero-day exploitation analysis**. Google Cloud Blog, [s.l.], 2025. Disponível em: https://cloud.google.com/blog/topics/threat-intelligence/2024-zero-day-trends. Acesso em: 11 jun. 2025.

CONDON, Caitlin. Rapid7 **Observed Exploitation of Critical MOVEit Transfer Vulnerability**. Rapid7 Blog, 1 jun. 2023. Disponível em: https://www.rapid7.com/blog/post/2023/06/01/rapid7-observed-exploitation-of-critical-moveit-transfer-vulnerability/. Acesso em: 6 out. 2025.
RBN TECNOLOGIA. **Pilares da segurança da informação**. RBN Tecnologia, 7 fev. 2022. Disponível em: https://rbntecnologia.com.br/pilares-da-seguranca-da-informacao/. Acesso em: 27 maio 2025.

COUTINHO, Mateus Micael; SANTOS, Robson Nunes dos; CUSTÓDIO, Vitor Henrique da Silva; AMARAL, Eliane Cristina; SABINO, Eliney; ABE, Narumi. **Estudo de caso: principais pilares da segurança da informação nas organizações**.

Gestão em Foco, Registro, v. 9, p. 489–500, 2017. Disponível em: https://portal.unisepe.com.br/unifia/wp-content/uploads/sites/10001/2018/06/052_estudo5.pdf. Acesso em: 27 maio 2025.

DAVID, Ori; TINKLENBERG, Sam; ZAVODCHIK, Maxim; HARPAZ, Ophir. **Dia zero (CVE-2023-34362) do MOVEit SQLi explorado pelo grupo de ransomware CL0P**. Akamai, [S.l.], 2023. Disponível em: <https://www.akamai.com/pt/blog/security-research/moveit-sqli-zero-day-exploit-clop-ransomware>. Acesso em: 6 out. 2025.

DELBIANCO, Natalia Rodrigues; SILVA, Edna Lúcia da. **Sociedade da informação e as mídias sociais no contexto da comunicação científica**. Revista ACB: Biblioteconomia em Santa Catarina, Florianópolis, v. 26, n. 3, p. 594-611, set./dez. 2021. Disponível em: https://www.researchgate.net/profile/Natalia-Rodrigues-Delbianco/publication/358060126_SOCIEDADE_DA_INFORMACAO_E_AS_MIDIAS_SOCIAIS_NO_CONTEXTO_DA_COMUNICACAO_CIENTIFICA/links/62e2959d4246456b55f0aadb/Sociedade-da-informacao-e-as-midias-sociais-no-contexto-da-comunicacao-cientifica.pdf. Acesso em: 6 out. 2025.

FERREIRA, Daniela Assis Alves. **Tecnologia: fator determinante no advento da sociedade de informação?** Perspectivas em Ciência da Informação, Belo Horizonte, v. 8, n. 1, p. 4–11, jan./jun. 2002. Disponível em: <https://periodicos.ufmg.br/index.php/pci/article/view/23455/18915>. Acesso em: 27 maio 2025.

FERREIRA, Lucas Vinicius Andrade. **Uma solução para gestão de vulnerabilidades de segurança da informação**. 2017. 43 f. Monografia (Especialização em Gestão de Segurança da Informação) - Universidade de Brasília, Brasília, 2017. Disponível em: <https://bdm.unb.br/bitstream/10483/30315/1/2017_LucasViniciusAndradeFerreira_tcc.pdf>. Acesso em: 6 out. 2025.

FIRST. **Common Vulnerability Scoring System SIG**. FIRST.org, [s.l.], 2025a. Disponível em: <https://www.first.org/cvss/>. Acesso em: 11 out. 2025.

FIRST. **Common Vulnerability Scoring System v3.1: specification document**. FIRST.org, [s.l.], 2025b. Disponível em: https://www.first.org/cvss/v3-1/specification-document. Acesso em: 11 out. 2025.

FONTES, Edison Luiz Gonçalves. **Políticas de segurança da informação**. Rio de Janeiro: RNP/ESR, 2015. Disponível em: < https://www.kufunda.net/publicdocs/Pol%C3%ADticas%20de%20seguran%C3%A7a%20da%20informa%C3%A7%C3%A3o%20(Edison%20Luiz%20Gon%C3%A7alves%20Fontes).pdf?utm_source=chatgpt.com>. Acesso em: 6 out. 2025.

GHELANI, Diptiben; HUA, Tan Kian; KODURU, Surendra Kumar Reddy. **Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking**. American Journal of Computer Science and Technology, v. 10, n. 1, p. 1-10, 2022.

Disponível em: <https://d197for5662m48.cloudfront.net/documents/publicationstatus/90319/preprint_pdf/87c34d475885f4f2b553401959b483cb.pdf?utm_source=chatgpt.com>. Acesso em: 27 mai. 2025.

GIL, Antônio Carlos. **Métodos e técnicas de pesquisa social**. 6. ed. São Paulo: Atlas, 2008. 732 p. Disponível em: https://ayanrafael.com/wp-content/uploads/2011/08/gil-a-c-mc3a9todos-e-tc3a9cnicas-de-pesquisa-social.pdf. Acesso em: 5 jun. 2025.

CHARRIER, Casey; SADOWSKI, James; LECIGNE, Clément; STOLYAROV, Vlad. **Hello 0-Days, My Old Friend: A 2024 Zero-Day Exploitation Analysis**. Google Cloud Blog, 29 abr. 2025. Disponível em: https://cloud.google.com/blog/topics/threat-intelligence/2024-zero-day-trends.

GUEYE, A.; GALHARDO, C. E. C.; BOJANOVA, I.; MELL, P. **A decade of reoccurring software weaknesses**. IEEE Security & Privacy, v. 19, n. 6, p. 38-47, 2021. Disponível em: https://pmc.ncbi.nlm.nih.gov/articles/PMC10021008/. Acesso em: 11 out. 2025.

GUO, Yang. **A review of Machine Learning-based zero-day attack detection: challenges and future directions**. Computer Communications, [S.l.], v. 198, p. 175–185, 2023. Disponível em: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=934769. Acesso em: 27 maio 2025.

IBM. **O que é a segurança da informação?** IBM, [S.l.], 2024. Disponível em: <https://www.ibm.com/br-pt/think/topics/information-security>. Acesso em: 6 out. 2025.

JANNUZZI, Celeste Aída Sirotheau Corrêa; SUGAHARA, Cibele Roberta; FALSARELLA, Orandi Mina. **Sistema de informação: um entendimento conceitual para a sua aplicação nas organizações empresariais**. Perspectivas em Ciência da Informação, v. 19, p. 94-117, 2014. Disponível em: https://www.scielo.br/j/pci/a/fKbBSPKSPdN6XbSkfyGMKMK/?format=pdf&lang=pt. Acesso em: 20 abr. 2024.

KASPERSKY. **O que é EDR? Definição de detecção e resposta de endpoint**. Kaspersky, 2025. Disponível em: https://www.kaspersky.com.br/resource-center/preemptive-safety/endpoint-detection-and-response. Acesso em: 9 jun. 2025.

KLETTENBERG, Josiane. **Segurança da informação: um estudo sobre o uso da engenharia social para obter informações sigilosas de usuários de instituições bancárias**. 2016. 181 f. Dissertação (Mestrado em Ciência da Informação) - Universidade Federal de Santa Catarina, Florianópolis, 2016. Disponível em: https://repositorio.ufsc.br/xmlui/bitstream/handle/123456789/172575/343623.pdf. Acesso em: 6 out. 2025.

KOHN, Karen; MORAES, Cláudia Herte de. **O impacto das novas tecnologias na sociedade: conceitos e características da Sociedade da Informação e da Sociedade Digital**. In: INTERCOM – Sociedade Brasileira de Estudos Interdisciplinares da Comunicação. XXX Congresso Brasileiro de Ciências da Comunicação, Santos, 29 de agosto a 2 de setembro de 2007. Anais… [S.l.], 2007. Disponível em: https://www.researchgate.net/publication/238065799_O_impacto_das_novas_tecnologias_na_sociedade_conceitos_e_caracteristicas_da_Sociedade_da_Informacao_e_da_Sociedade_Digital1. Acesso em: 27 maio 2025.

KOSKENKORVA, H. **The role of security patch management in vulnerability management**. 2021. 79 f. Dissertação (Mestrado em Cybersecurity) – Jamk University of Applied Sciences, Jyväskylä, 2021. Disponível em: https://www.theseus.fi/bitstream/handle/10024/511059/Koskenkorva_Helena.pdf?sequence=2&isAllowed=y. Acesso em: 20 out. 2025.

KUTSOVSKY, Misha. **Windows Defender Exploit Guard: reduce the attack surface against next generation malware**. Microsoft Security Blog, Redmond, 23 out. 2017. Disponível em: https://www.microsoft.com/en-us/security/blog/2017/10/23/windows-defender-exploit-guard-reduce-the-attack-surface-against-next-generation-malware/. Acesso em: 6 jun. 2025.

LAURINDO, Fernando José Barbin; SHIMIZU, Tamio; CARVALHO, Marly Monteiro de; RABECHINI JR., Roque. **O papel da tecnologia da informação (TI) na estratégia das organizações**. Gestão & Produção, São Carlos, v. 8, n. 2, p. 160–179, ago. 2001. Disponível em: https://www.scielo.br/j/gp/a/vt5SZnMwqNVyxFnkvJnLXCH/?format=pdf&lang=pt. Acesso em: 27 maio 2025.

LEMES, Denise Fernandes Neves; PAVANI, Guilherme Cintra; SALES, Rafael Marcos; LOPES, Tatiana Schmitz de Almeida. **A segurança da informação de encontro às conformidades da LGPD**. Revista Perspectiva em Gestão & Conhecimento, Praia Grande, v. 13, n. 2, p. 104-120, 2023. Disponível em: https://www.fatecpg.edu.br/revista/index.php/ps/article/view/171/242. Acesso em: 7 out. 2025.

LIMA, Erick Amaro Dutra de. **Práticas para mitigar ataques cibernéticos em sistemas de telecomunicações: estudo de caso**. 2024. Trabalho de Conclusão de Curso (Tecnólogo em Sistemas de Telecomunicações) – Instituto Federal de Educação, Ciência e Tecnologia da Paraíba, Campus João Pessoa, João Pessoa, 2024. Disponível em: https://repositorio.ifpb.edu.br/bitstream/177683/4012/1/TCC-%20Erick%20Amaro%20Dutra%20de%20Lima.pdf. Acesso em: 27 maio 2025.

MALERBA, César. Vulnerabilidades e Exploits: técnicas, detecção e prevenção. 2010. Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação) – Universidade Federal do Rio Grande do Sul, Porto Alegre, 2010. Disponível em:

https://lume.ufrgs.br/bitstream/handle/10183/26337/00757768.pdf?sequence=1. Acesso em: 27 maio 2025.

MICROSOFT. **O que é arquitetura de confiança zero?** Microsoft Segurança, 2024. Disponível em: https://www.microsoft.com/pt-br/security/business/security-101/what-is-zero-trust-architecture. Acesso em: 27 maio 2025.

MITRE CORPORATION. Common vulnerabilities and exposures (CVE). CVE.org, [s.l.], [2025]. Disponível em: https://www.cve.org/About/Overview. Acesso em: 11 out. 2025.

MOREIRA, Guilherme Baesso; CALEGARIO, Vanusa Menditi; DUARTE, Julio Cesar; SANTOS, Anderson F. Pereira dos. **A era dos Crypto Ransomwares: um estudo de caso sobre o WannaCry**. In: XVII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg 2017). Rio de Janeiro: Sociedade Brasileira de Computação, 2017. p. 509–516. Disponível em: https://sol.sbc.org.br/index.php/sbseg/article/download/19525/19353/. Acesso em: 27 maio 2025.

MORESI, E. A. D. **Delineando o valor do sistema de informação de uma organização**. Ciência da Informação, 29(1), p. 14-21, 2000. Disponível em: https://www.scielo.br/j/ci/a/pzj7MLqJc6jX5zHLxH5PFwq/?format=pdf&lang=pt.

NARANG, Satnam. **CVE-2023-34362: MOVEit Transfer critical zero-day vulnerability exploited in the wild**. Tenable Blog, [S.l.], 2023. Disponível em: https://www.tenable.com/blog/cve-2023-34362-moveit-transfer-critical-zero-day-vulnerability-exploited-in-the-wild.

NIST. **Guide to enterprise patch management planning:** preventive maintenance for technology. Gaithersburg: NIST, 2022. (NIST Special Publication ; 800-40, rev. 4). Disponível em: https://doi.org/10.6028/NIST.SP.800-40r4.

OLIVEIRA, Beatriz Martins de; WALDMAN, Ricardo Libel. **Conceitos de informação e sociedade da informação e sua importância**. Meritum, Belo Horizonte, v. 15, n. 4, p. 247-263, set. 2021. Disponível em: https://revista.fumec.br/index.php/meritum/article/view/7965. Acesso em: 6 out. 2025.

OWASP. Vulnerabilities. OWASP Community, [s.l.], [2025]. Disponível em: https://owasp.org/www-community/vulnerabilities/. Acesso em: 11 out. 2025.

PELTIER, Thomas R. **Information Security Risk Analysis**. 2. ed. Boca Raton: Auerbach Publications, 2005.

PINHEIRO, José Maurício dos Santos. **Ameaças e ataques aos sistemas de informação: prevenir e antecipar**. Cadernos UniFOA, Volta Redonda, v. 3, n. 5, p.

11-21, mar. 2017. Disponível em: <https://revistas.unifoa.edu.br/cadernos/article/view/885>. Acesso em: 6 out. 2025.

PRICE, Sean M. **Extending the McCumber Cube to Model Network Defense**. ISSA Journal, [S.l.], p. 1-18, set. 2008. Disponível em: https://content.bellevue.edu/cst/cis/312/Documents/mccumber_article.pdf. Acesso em: 6 out. 2025.

ROCHA, Miguel Sanches. **Identificação de ataques não-conhecidos em sistemas de detecção de intrusão baseados em anomalia**. 2023. Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação) – Universidade Federal de Uberlândia, Uberlândia, 2023. Disponível em: https://repositorio.ufu.br/bitstream/123456789/38147/1/Identifica%C3%A7%C3%A3oDeAtaques.pdf. Acesso em: 27 maio 2025.

ROMAR, A.; SILVA, B. **Sistema de detecção de ransomware utilizando inteligência artificial**. 2022. Trabalho de Conclusão de Curso (Tecnólogo em Análise e Desenvolvimento de Sistemas) – Universidade Presbiteriana Mackenzie, Faculdade de Computação e Informática, São Paulo, 2022. Disponível em: https://dspace.mackenzie.br/bitstreams/76fdc418-b71d-45f0-9ebb-c01b1cdbc833/download. Acesso em: 12 nov. 2025.

SANTOS, Guilherme Alves dos. **LGPD: a responsabilidade civil do fornecedor perante o vazamento de dados**. Jusbrasil, [S.l.], 2025. Disponível em: <https://www.jusbrasil.com.br/artigos/lgpd-a-responsabilidade-civil-do-fornecedor-perante-o-vazamento-de-dados/2026022326>. Acesso em: 6 out. 2025.

SASS, Simeão Donizeti. **A tecnologia no mundo contemporâneo**. 2015. Disponível em: https://www.sfu.ca/~andrewf/10_A%20tecnologia%20no%20mundo.pdf. Acesso em: 26 maio 2025.

SILVA, Pedro José da; NASCIMENTO, Renata. **A segurança da informação de encontro às conformidades da LGPD**. Revista Produção e Saberes, v. 3, n. 2, p. 1–10, 2022. Disponível em: https://www.fatecpg.edu.br/revista/index.php/ps/article/view/171/242. Acesso em: 27 maio 2025.

STALLINGS, William; BROWN, Lawrie. **Computer security: principles and practice**. 4. ed. Harlow: Pearson Education Limited, 2018. Disponível em: https://api.pageplace.de/preview/DT0400.9781292220635_A37747428/preview-9781292220635_A37747428.pdf. Acesso em: 6 out. 2025.

STAIR, Ralph M.; REYNOLDS, George W. **Principles of Information Systems: A Managerial Approach**. 9. ed. Boston: Cengage Learning, 2009. ISBN 978-0324665284.

SYMBIOTI. **Entenda quais são os três pilares da segurança da informação**. Symbioti, [S.l.], 2025. Disponível em: https://www.symbioti.com.br/entenda-quais-sao-os-tres-pilares-da-seguranca-da-informacao/. Acesso em: 6 out. 2025.

TECHNOLOGIES, SANGFOR. **How to prevent zero-day attacks?** Sangfor Glossary, [s.l.], [2025]. Disponível em: https://www.sangfor.com/glossary/cybersecurity/how-to-prevent-zero-day-attacks. Acesso em: 20 out. 2025.

TI INSIDE. **Brasil deve investir R$ 104,6 bi em cibersegurança até 2028, aponta relatório**. São Paulo, 23 jul. 2025. Disponível em: <https://tiinside.com.br/23/07/2025/brasil-deve-investir-r-1046-bi-em-ciberseguranca-ate-2028-aponta-relatorio/>. Acesso em: 6 out. 2025.

TI INSIDE. **Cibersegurança é prioridade para mais de 80% das empresas de médio porte do Brasil**. São Paulo, 6 maio 2024. Disponível em: <https://tiinside.com.br/06/05/2024/ciberseguranca-e-prioridade-para-mais-de-80-das-empresas-de-medio-porte-do-brasil/>. Acesso em: 6 out. 2025.

VALE, Fábio do; BELCHIOR, Natália Barbosa; NASCIMENTO, Weverton Gomes do; YASSUMOTO, Marcel Ferreira. **A segurança digital nas pequenas e médias empresas**: desafios e possíveis soluções. Revista Latino-Americana de Estudos Científicos, v. 3, n. 16, 2022. Disponível em: < https://periodicos.ufes.br/ipa/article/view/38919?utm_source>. Acesso em: 26 maio 2025.

WEBSTER, Frank. **Theories of the Information Society**. 3. ed. Londres: Routledge, 1993. Disponível em: <https://bayanbox.ir/view/1597312676074457092/mediajournal.ir-910051.pdf>. Acesso em: 26 maio 2025.

WERTHEIN, Jorge. **A sociedade da informação e seus desafios**. Ciência da Informação, Brasília, v. 29, n. 2, p. 71–77, maio/ago. 2000. Disponível em: <https://www.scielo.br/j/ci/a/rmmLFLLbYsjPrkNrbkrK7VF/?format=pdf&lang=pt>. Acesso em: 27 maio 2025.