REVISTA TECNOLÓGICA – uniFATEC
ISSN: 2179-3778
DOI: 10.62790/rtfv17n1-003

Submitted: Jul 13th, 2026
Approved: Aug 3rd, 2026

Priorização inteligente de vulnerabilidades: uma abordagem baseada em perfis de risco descobertos com machine learning

Intelligent vulnerability prioritization: a machine learning-based approach to discovering risk profiles

Priorización inteligente de vulnerabilidades: un enfoque basado en aprendizaje automático para descubrir perfiles de riesgo

Madson Luiz Magno da Silva
Mestrando em Engenharia Elétrica
Instituição: Universidade de Brasília (UNB)
Endereço: Brasília, Distrito Federal, Brasil
E-mail: silva.madson@aluno.unb.br

João Souza Neto
Pós-Doc em Segurança Cibernética
Instituição: Universidade de Brasília (UNB)
Endereço: Brasília, Distrito Federal, Brasil
E-mail: neto.joao@unb.br

Rafael Rabelo Nunes
Doutor em Engenharia Elétrica
Instituição: Universidade de Brasília (UNB)
Endereço: Brasília, Distrito Federal, Brasil
E-mail: rafaelrabelo@unb.br

Helton Garcia
Mestre em Engenharia Elétrica
Instituição: Universidade de Brasília (UNB)
Endereço: Brasília, Distrito Federal, Brasil
E-mail: heltongarcia@gmail.com

RESUMO
O crescimento contínuo do número de vulnerabilidades de software torna inviável tratá-las apenas com base em métricas de severidade técnica, como o Common Vulnerability Scoring System (CVSS), o que pode levar a decisões de remediação desalinhadas com o risco real ao negócio. Este trabalho aborda essa lacuna ao propor uma abordagem de priorização de vulnerabilidades orientada a perfis de risco, que combina a probabilidade de exploração, medida pelo Exploit Prediction Scoring System (EPSS), com o impacto contextual dos ativos, representado pela Nota de Criticidade de Sistema (NCS). A metodologia enriquece um conjunto de vulnerabilidades com essas métricas e aplica técnicas de clusterização para identificar grupos com padrões distintos de risco, permitindo comparar a priorização tradicional com a priorização baseada em risco real. Os resultados evidenciam perfis de vulnerabilidades que não seriam percebidos apenas

pela severidade técnica, além de mostrar que é possível reduzir significativamente o conjunto de itens tratados como prioritários, mantendo foco nas ameaças de maior relevância. Como contribuição prática, a abordagem oferece às equipes de segurança uma visão estratégica para planejar remediações mais eficientes, alinhadas à criticidade dos ativos e à probabilidade de exploração.

Palavras-chave: aprendizado de máquina, clusterização, gestão de risco, priorização de vulnerabilidades.

ABSTRACT

The continuous growth in the number of software vulnerabilities makes it unfeasible to handle them only by technical severity metrics, such as Common Vulnerability Scoring System (CVSS), which may lead to remediation decisions misaligned with the real business risk. This work addresses this gap by proposing a vulnerability prioritization approach guided by risk profiles that combines the probability of exploitation, measured by the Exploit Prediction Scoring System (EPSS), with the contextual impact of assets, represented by the System Criticality Score (NCS). The methodology enriches a vulnerability dataset with these metrics and applies clustering techniques to identify groups with distinct risk patterns, allowing the comparison between traditional prioritization and real-risk-based prioritization. The results reveal vulnerability profiles that would not be perceived by technical severity alone and show that it is possible to significantly reduce the set of items treated as priority while keeping the focus on the most relevant threats. As a practical contribution, the approach offers security teams a strategic view to plan more efficient remediation actions, aligned with asset criticality and exploitation probability.

Keywords: clustering, machine learning, risk management, vulnerability prioritization.

RESUMEN

El continuo aumento del número de vulnerabilidades de software hace inviable abordarlas únicamente mediante métricas de gravedad técnica, como el Sistema Común de Puntuación de Vulnerabilidades (CVSS), lo que puede derivar en decisiones de remediación desalineadas con el riesgo real para el negocio. Este trabajo aborda esta brecha proponiendo un enfoque de priorización de vulnerabilidades guiado por perfiles de riesgo que combina la probabilidad de explotación, medida por el Sistema de Puntuación de Predicción de Explotación (EPSS), con el impacto contextual de los activos, representado por la Puntuación de Criticidad del Sistema (NCS). La metodología enriquece un conjunto de datos de vulnerabilidades con estas métricas y aplica técnicas de agrupamiento para identificar grupos con patrones de riesgo distintos, lo que permite comparar la priorización tradicional con la basada en el riesgo real. Los resultados revelan perfiles de vulnerabilidad que no se percibirían solo con la gravedad técnica y demuestran que es posible reducir significativamente el conjunto de elementos considerados prioritarios, manteniendo el enfoque en las amenazas más relevantes. Como contribución práctica, el enfoque ofrece a los equipos de seguridad una perspectiva estratégica para planificar acciones de remediación más eficientes, alineadas con la criticidad de los activos y la probabilidad de explotación.

Palabras clave: agrupación, aprendizaje automático, gestión de riesgos, priorización de vulnerabilidades.

1 INTRODUÇÃO

A gestão de vulnerabilidades é um processo essencial da segurança da informação, pois novas falhas em softwares, sistemas e dispositivos são descobertas continuamente, gerando um fluxo de exposições que precisa ser tratado com recursos limitados. Nessa realidade, a priorização baseada apenas na severidade técnica calculada pelo Common Vulnerability Scoring System (CVSS) mostra-se insuficiente, porque desconsidera o contexto do ativo e a probabilidade de exploração, podendo levar a decisões desalinhadas com o risco real ao negócio (Spring, 2021).Para mitigar essas limitações, a adoção de métricas dinâmicas como o *Exploit Prediction Scoring System* (EPSS) introduziu a dimensão de probabilidade ao cálculo de risco (Jacobs *et al*., 2021). No entanto, a disponibilidade de dados multidimensionais impõe um novo desafio: qual técnica algorítmica é mais adequada para processar esses dados e gerar decisões de segurança confiáveis?

Neste trabalho, o risco real é entendido como um risco contextualizado, resultante da combinação entre a probabilidade de exploração de uma vulnerabilidade e o impacto que seu comprometimento causa nos ativos e processos da organização, em consonância com princípios de gestão de risco como os da ISO/IEC 27005 (International Organization for Standardization, 2022). Essa perspectiva reconhece que vulnerabilidades de alta severidade técnica podem representar baixo risco quando associadas a ativos pouco críticos ou com baixa chance de exploração, enquanto falhas de severidade moderada em sistemas críticos podem demandar maior prioridade.

Para abordar essa lacuna, o artigo propõe uma abordagem de priorização baseada em perfis de risco, construída com técnicas de machine learning não supervisionado. O método enriquece um conjunto de vulnerabilidades com a probabilidade de exploração estimada pelo Exploit Prediction Scoring System (EPSS) (FIRST, 2024) e com a Nota de Criticidade de Sistema (NCS), calculada a partir do Framework de Privacidade e Segurança da Informação (PPSI) (MGI, 2024), e aplica algoritmos de clusterização para agrupar vulnerabilidades em perfis com padrões distintos de risco. O objetivo geral é desenvolver e avaliar essa abordagem, incrementando um dataset com métricas de probabilidade (EPSS) e impacto (NCS), identificando perfis de risco e analisando suas características para apoiar estratégias de remediação mais eficientes.

1.1 OBJETIVOS

O objetivo geral deste trabalho é propor uma abordagem de priorização de vulnerabilidades corporativas baseada em perfis de risco contextuais, utilizando algoritmos de aprendizado de máquina não supervisionado para segmentar ameaças de forma acionável.

Para atingir o objetivo principal, foram definidos os seguintes objetivos específicos:

a) enriquecer um conjunto de dados de vulnerabilidades com a probabilidade de exploração obtida via Exploit Prediction Scoring System (EPSS) e com o impacto no negócio medido pela Nota de Criticidade de Sistema (NCS);
b) aplicar o algoritmo K-Means para identificar a quantidade ideal de agrupamentos de risco e categorizar as vulnerabilidades em perfis de criticidade;
c) utilizar o algoritmo DBSCAN para detectar anomalias estatísticas e vulnerabilidades atípicas de interesse para análise individualizada;
d) comparar a eficiência operacional do modelo proposto em relação ao método de priorização tradicional fundamentado exclusivamente no Common Vulnerability Scoring System (CVSS), mensurando a redução no volume de alertas prioritários.

2 REFERENCIAL TEÓRICO E TRABALHOS RELACIONADOS

Para fundamentar a análise comparativa proposta, esta seção apresenta as métricas de risco utilizadas e os algoritmos de clusterização avaliados, seguida pela discussão dos trabalhos correlatos que motivaram este estudo.

2.1 FUNDAMENTAÇÃO TEÓRICA

A gestão de vulnerabilidades é um desafio central na cibersegurança, impulsionado por um crescimento exponencial no número de falhas descobertas. O sistema Common Vulnerabilities and Exposures (CVE), mantido pela MITRE Corporation, é o padrão global para identificar e catalogar essas falhas. Segundo a base de CVEs, em 2023, foram publicadas mais de 29.000 novas vulnerabilidades. E em 2024, esse número ultrapassou 40.000. O volume de novos CVEs registrados neste ano de 2025,

de janeiro até julho, é de mais de 26.000 vulnerabilidades (CVEDetails, 2025), um número que torna a remediação de todas as falhas identificadas uma tarefa impraticável para a maioria das organizações.

Para lidar com esse volume, a indústria adotou o CVSS como principal métrica para avaliar a severidade técnica de um CVE, gerando uma nota de 0.0 a 10.0 (FIRST.org, 2019). Contudo, a dependência exclusiva do CVSS para priorização possui limitações, pois sua natureza estática ignora a probabilidade de exploração e sua abordagem agnóstica ao ambiente ignora o impacto contextual da falha no negócio, resultando em uma priorização muitas vezes ineficaz (Spring, 2021).

Uma abordagem mais robusta se baseia em princípios de gestão de risco, definidos por padrões como a ISO 27005, como uma função da probabilidade de um evento e do seu impacto nos objetivos da organização (International Organization for Standardization, 2022).

Uma das métricas utilizadas para superar as limitações do CVSS na avaliação da probabilidade de exploração é o EPSS (Exploit Prediction Scoring System). Trata-se de um modelo aberto, baseado em Machine Learning, que calcula a probabilidade (em uma escala de 0 a 1) de uma vulnerabilidade específica (CVE) ser explorada ativamente nos próximos 30 dias, utilizando dados de threat intelligence (FIRST.org, 2024).

Para a avaliação do impacto contextual, o Framework de Privacidade e Segurança da Informação (PPSI) do governo brasileiro define uma metodologia para calcular a Nota de Criticidade de Sistema (NCS). Esta métrica, baseada em um modelo de avaliação proposto pelo Tribunal de Contas da União (Tribunal de Contas da União, 2020), quantifica a importância de um sistema (ativo) para a organização, considerando critérios relacionados ao negócio (como danos financeiros, reputacionais, etc.), resultando em uma pontuação que reflete o impacto caso o sistema seja comprometido (MGI, 2024).

Na mesma linha, frameworks baseados em regras e árvores de decisão, como o SSVC (Howard *et al*., 2025), guiam o analista através de um fluxo de decisão estruturado para categorizar a vulnerabilidade com base no contexto específico do stakeholder. Enquanto frameworks como o SSVC++ guiam a categorização através de um fluxo de decisão pré-definido, a abordagem de clusterização adotada neste trabalho busca descobrir automaticamente os perfis de risco emergentes a partir dos padrões nos dados, oferecendo uma taxonomia potencialmente mais adaptada ao ambiente específico.

2.2 TRABALHOS CORRELATOS

Os métodos de priorização atuais que se baseiam apenas em CVSS enfrentam dificuldades como a fadiga de alertas e a má alocação de recursos (Spring, 2021). Para enfrentar esses desafios, a literatura acadêmica tem explorado o uso de ciência de dados para a gestão de vulnerabilidades. Diversos pesquisadores têm aplicado aprendizado supervisionado para aprimorar a priorização, utilizando, por exemplo, modelos de classificação para prever a probabilidade de exploração (Jacobs *et al*., 2023) e modelos de regressão para gerar pontuações de risco dinâmicas e mais completas (Althar *et al*., 2022).

Outras abordagens buscam estruturar a decisão de priorização sem depender exclusivamente de modelos preditivos. Frameworks baseados em fluxos de decisão, como o SSVC (Stakeholder-Specific Vulnerability Categorization) (Spring *et al*., 2021), guiam a categorização de vulnerabilidades por meio de uma árvore de decisão que considera fatores como estado da exploração, impacto técnico e o contexto específico do stakeholder, resultando em ações recomendadas (e.g., agir, atender, rastrear).

Diferentemente das abordagens supervisionadas, que buscam prever um valor ou classe, este trabalho explora o potencial da clusterização não supervisionada para descobrir os perfis de risco inerentes aos dados. A técnica k-Means, originalmente proposta por MacQueen (1967), é um algoritmo de particionamento que agrupa vulnerabilidades com base na sua similaridade em um espaço de risco. Sua eficiência e simplicidade continuam a torná-la uma escolha relevante para a análise de dados em larga escala, com aplicações recentes em cibersegurança e medição de riscos, conforme corroborado por estudos comparativos que destacam sua robustez na identificação de padrões (Fuhnwi *et al*., 2023; Al Mamun *et al*., 2024; Val *et al*., 2025).

A utilização da média para caracterizar os centroides é uma propriedade intrínseca ao funcionamento do algoritmo k-Means. O objetivo do algoritmo é particionar os dados de forma a minimizar a soma das distâncias quadráticas intra-cluster (WCSS), e o ponto que minimiza essa soma para qualquer grupo de dados é o seu centroide, definido como a média de todos os pontos pertencentes àquele cluster (James *et al*., 2021).

Como método complementar de validação e identificação de anomalias, utiliza-se o DBSCAN (Density-Based Spatial Clustering of Applications with Noise), um algoritmo baseado em densidade de vetores capaz de encontrar clusters de formatos arbitrários e

identificar outliers (Ester *et al*., 1996). A capacidade do DBSCAN de isolar ruídos o torna uma ferramenta valiosa para a descoberta de anomalias em conjuntos de dados de segurança (Goswami, 2024), sendo frequentemente empregado em estudos empíricos para validar ou contrastar os agrupamentos encontrados por métodos representativos como o k-Means (Fuhnwi *et al*., 2023).

O DBSCAN classifica como 'ruído' (Ester *et al*., 1996) os pontos que não possuem um número mínimo de vizinhos próximos dentro de um raio pré-definido, indicando que se encontram em regiões esparsas do espaço de risco. Essa capacidade de identificar e rotular explicitamente pontos de ruído é uma característica fundamental do DBSCAN e o principal motivo de sua aplicação na detecção de anomalias, como explorado em estudos empíricos recentes (Fuhnwi *et al*., 2023).

Além da natureza dos clusters que cada algoritmo é capaz de encontrar, a literatura aponta a complexidade computacional e a escalabilidade como fatores críticos na escolha de um método para aplicação em larga escala. Algoritmos como o k-Means são reconhecidos por sua eficiência e escalabilidade. Sua complexidade computacional é linear em relação ao número de entradas no dataset, o que garante sua viabilidade em conjuntos de dados com dezenas de milhares de entradas, desde que o número de clusters e as dimensões não sejam excessivamente grandes (Pant *et al*., 2025).

Em contraste, estudos recentes confirmam que alternativas como o DBSCAN, apesar de suas vantagens, podem apresentar limitações de desempenho e consumo de memória em grandes volumes de dados, um fator crucial para a aplicação prática em ambientes corporativos (Fuhnwi *et al*., 2023).

3 METODOLOGIA

A presente pesquisa foi delineada com base em uma abordagem metodológica mista, que combina procedimentos quantitativos e qualitativos para atingir seus objetivos.

Quanto à sua natureza, esta pesquisa se classifica como aplicada, pois visa gerar conhecimentos para a aplicação prática na resolução do problema específico de priorização de vulnerabilidades em ambientes corporativos (Marconi, 2017; Lakatos, 2017). No que tange aos objetivos, a pesquisa é de caráter exploratório e descritivo, buscando proporcionar maior familiaridade e um novo entendimento sobre o problema

ao investigar o uso de métricas de risco contextuais e técnicas de Machine Learning na priorização de vulnerabilidades (Marconi, 2017; Lakatos, 2017).

A abordagem do problema é tanto quantitativa, na manipulação e análise estatística dos dados de vulnerabilidades, quanto qualitativa, na interpretação e nomeação dos perfis de risco (clusters) gerados pelos algoritmos. Os procedimentos técnicos envolveram a pesquisa bibliográfica para a fundamentação teórica sobre CVSS, EPSS e algoritmos de clusterização, e um estudo de caso simulado para a aplicação e validação dos modelos propostos, conforme preconizam as boas práticas de pesquisa científica (Marconi, 2017; Lakatos, 2017).

4 RESULTADOS E DISCUSSÃO

Nesta seção, são apresentados os resultados da aplicação das metodologias de clusterização.

4.1 PROCEDIMENTO EXPERIMENTAL

4.1.1 Geração e enriquecimento do Dataset

O ponto de partida foi a geração de um dataset simulado, representativo do ambiente de uma organização. O processo de geração de dados envolveu:

A coleta de dados brutos foi feita a partir da utilização de um relatório de varredura e associação simulada de seus alertas a identificadores de vulnerabilidades (CVEs) da base National Vulnerability Database (NVD).

A obtenção da dimensão de Impacto através do cálculo da Nota de Criticidade de Sistema (NCS) para cada ativo envolveu a aplicação da fórmula NC = (2 * I) + V, conforme a metodologia PPSI (MGI, 2024) baseada no modelo TCU (Tribunal de Contas da União 2020), utilizando como entrada as avaliações de Impacto (I) e Vulnerabilidade (V) de cada sistema.

Para garantir a relevância estatística e evitar que ativos com um número excessivo de vulnerabilidades dominassem o conjunto, foi aplicada uma técnica de balanceamento por amostragem aleatória com limite superior variável. Para cada ativo com mais de 50 vulnerabilidades, um limite máximo entre 50 e 250 foi sorteado, e uma amostra aleatória

(random_state=42), sem ordenação prévia por CVSS, foi selecionada. Ativos com 50 ou menos vulnerabilidades foram mantidos integralmente.

O dataset balanceado foi então enriquecido com os scores EPSS, obtidos da base pública do FIRST.org (FIRST.org, 2024) e associados via CVE. Vulnerabilidades sem score EPSS correspondente receberam o valor 0.

4.1.2 Pré-processamento

O dataset final, contendo as features EPSS e NCS, passou por uma etapa final de pré-processamento. Foi aplicado o StandardScaler (biblioteca Scikit-learn) para padronizar os atributos (média 0 e desvio padrão 1), garantindo que ambas as métricas tivessem a mesma importância nos cálculos de distância dos algoritmos.

4.1.3 Modelagem e análise comparativa

Com o dataset pré-processado, foram aplicados três algoritmos de clusterização com lógicas distintas:

K-Means: Foi selecionado como o algoritmo de particionamento principal, devido à sua interpretabilidade e baixa complexidade computacional, o que garante sua escalabilidade (Jain, 2010; MacQueen, 1967).

Clusterização Hierárquica: Foi aplicada a abordagem aglomerativa como ferramenta exploratória para gerar um dendrograma, auxiliando visualmente na validação da estrutura dos dados (James *et al.*, 2013).

DBSCAN: Foi empregado como método complementar baseado em densidade (Ester *et al.*, 1996), com o duplo propósito de validar o número de clusters de alta densidade encontrados e, principalmente, identificar vulnerabilidades anômalas (outliers) (Fuhnwi *et al.*, 2023).

4.1.4 Definição de parâmetros

Para suportar a escolha de k dentro para o K-Means, o Método do Cotovelo (WCSS) foi usado para analisar a variância intra-cluster e sugerir um valor ótimo para k. A análise Visual do Dendrograma foi usada qualitativamente para corroborar a estrutura

de agrupamento.

4.1.5 Ambiente experimental

A execução dos algoritmos e todas as análises de dados foram realizadas em um ambiente com as seguintes especificações: processador Intel(R) Core(TM) i5-6500T @ 2.50GHz, 8,00 GB de RAM e sistema operacional Windows 11 Pro, utilizando a linguagem Python e bibliotecas como Pandas, Scikit-learn e Matplotlib.

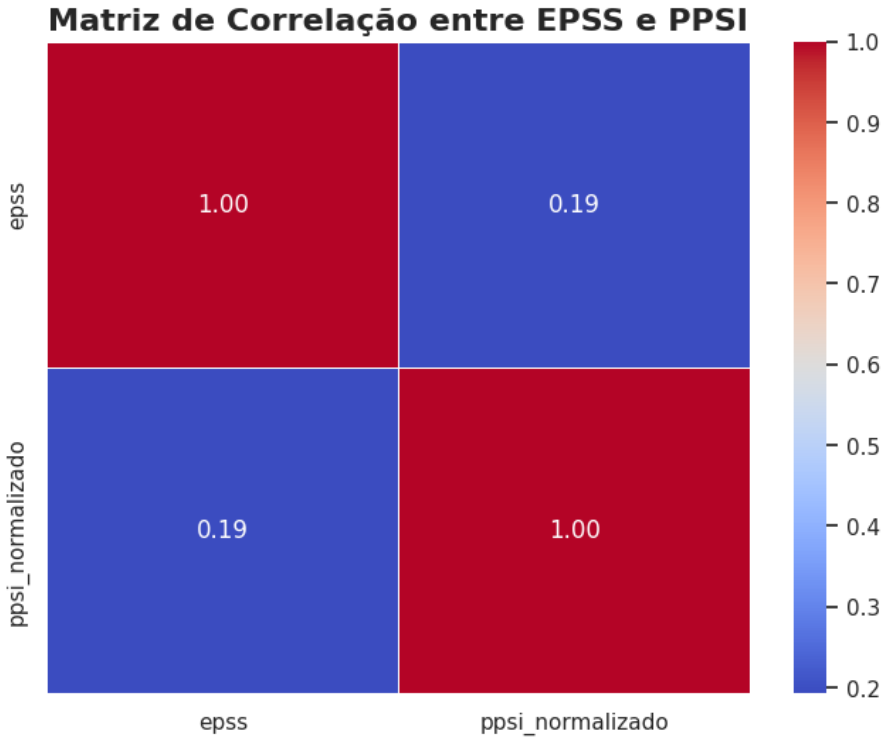
4.2 ANÁLISE EXPLORATÓRIA DE DADOS (EDA)

Antes da aplicação dos modelos de clusterização, realizou-se uma Análise Exploratória de Dados (EDA), proposta originalmente por Tukey (1977) que continua sendo uma etapa fundamental na análise de dados moderna, permitindo a investigação e sumarização das principais características do dataset antes da modelagem formal (James *et al*., 2021), com o objetivo de investigar as características e as relações entre as principais características de risco do dataset: a probabilidade de exploração (EPSS) e o impacto contextual no negócio (NCS). O objetivo desta análise foi validar a hipótese de que estas métricas representam dimensões de risco distintas e que sua combinação revela a existência de agrupamentos inerentes aos dados, ou seja, que os pontos não se distribuem de forma aleatória, mas formam concentrações distintas, justificando assim o uso de técnicas de Machine Learning para identificar formalmente esses grupos.

4.2.1 Análise de correlação das métricas de risco

A primeira etapa da análise consistiu em medir a relação linear entre as variáveis de risco utilizando o coeficiente de correlação de Pearson (James *et al*., 2013). A matriz de correlação resultante, apresentada na Figura 1, quantifica o grau de interdependência entre o EPSS e o NCS.

Figura 1 – Análise de Correlação entre a Probabilidade de Exploração (EPSS) e o Impacto no Negócio (NCS).



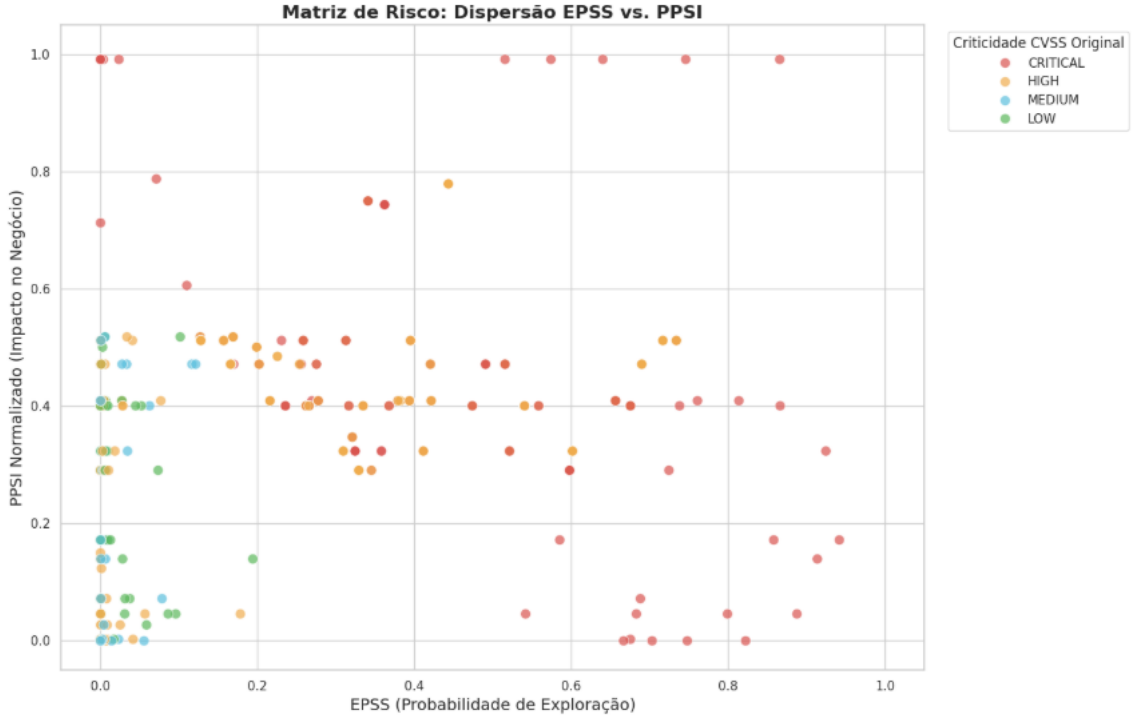
Fonte: Autoria própria (2026).

A análise da matriz na Figura 1 revela um coeficiente de correlação baixo e próximo de zero entre as duas métricas. Este resultado é fundamental para a proposição deste trabalho, pois comprova empiricamente que a probabilidade de uma vulnerabilidade ser explorada não possui uma relação linear direta com a criticidade do ativo onde ela reside. A independência estatística entre as variáveis valida a premissa de que o NCS captura o componente de impacto no negócio do risco, enquanto o EPSS captura o componente de probabilidade de exploração, sendo ambas dimensões complementares e necessárias para uma avaliação de risco.

4.2.2 Visualização da matriz de risco

Para visualizar a interação entre as duas métricas de risco, foi gerado um gráfico de dispersão dessa Matriz de Risco, posicionando cada vulnerabilidade de acordo com suas pontuações de EPSS (eixo X) e NCS (eixo Y), conforme a Figura 2.

Figura 2 – Matriz de Risco: Dispersão entre EPSS e NCS.



Fonte: Autoria própria (2026).

A análise do gráfico de dispersão apresentado na Figura 2 evidencia que as vulnerabilidades não se distribuem de maneira uniforme, sugerindo a presença de agrupamentos.

Uma análise quantitativa da distribuição, particionando o gráfico em quadrantes a partir do ponto central (0.5 para cada eixo), confirma a magnitude dessa heterogeneidade. Verifica-se que o quadrante inferior esquerdo (baixo EPSS e baixo PPSI), representativo de menor risco, concentra a maioria dos dados, com 294 das 421 vulnerabilidades (aproximadamente 70% do total).

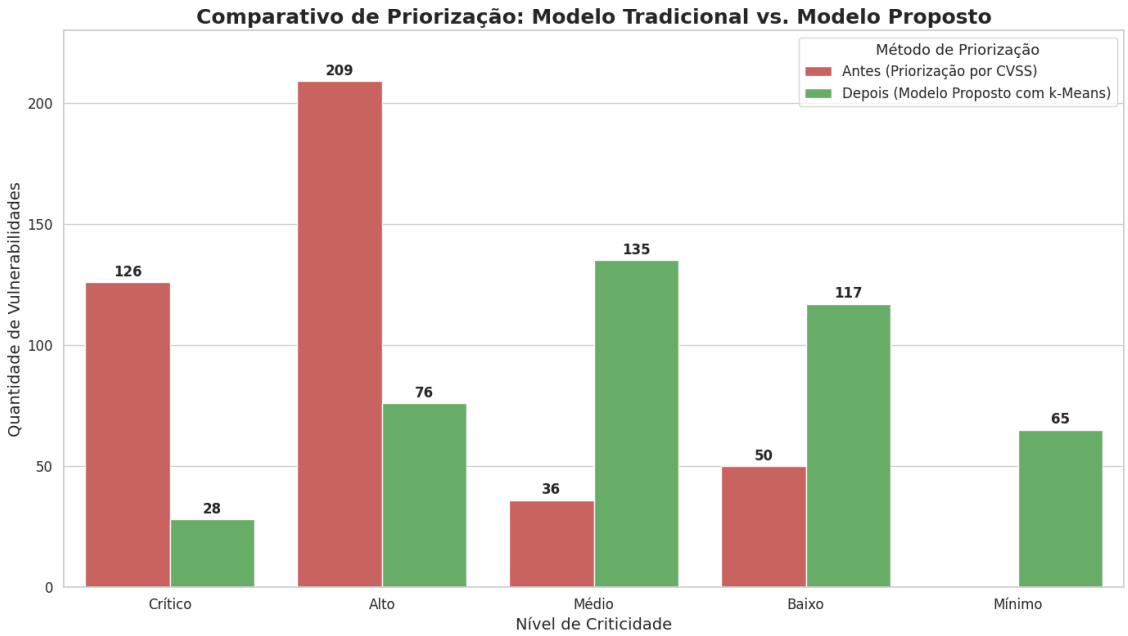
Em contrapartida, os quadrantes que representam riscos assimétricos são mais esparsos: o superior esquerdo (baixo EPSS, alto PPSI) contém 92 vulnerabilidades (22%), enquanto o inferior direito (alto EPSS, baixo PPSI) abrange 23 (5,5%). A região de maior criticidade potencial, o quadrante superior direito (alto EPSS, alto PPSI), é a menos populosa, com somente 12 pontos de dados (2,9%).

Essa distribuição desigual, confirmada de forma quantitativa, indica a existência de uma estrutura de agrupamentos dos dados e justifica a aplicação de algoritmos de clusterização para a identificação e caracterização formal desses perfis de risco.

4.3 COMPARATIVO DE PRIORIZAÇÃO E IMPACTO DO MODELO

A aplicação da metodologia proposta resulta em uma reclassificação do cenário de risco, cujo impacto prático é demonstrado na Figura 3, a qual compara diretamente a distribuição de vulnerabilidades por nível de criticidade antes ('Priorização por CVSS') e depois da aplicação do modelo ('Modelo Proposto com k-Means').

Figura 3 – Comparativo: Modelo Tradicional (CVSS) vs. Modelo Proposto (k-Means)



Fonte: Autoria própria (2026).

A principal consequência observada é a redução no volume de alertas de alta prioridade. Somando-se as categorias 'Crítico' e 'Alto', o modelo tradicional identifica 335 vulnerabilidades que exigiriam atenção imediata. Em contrapartida, o modelo proposto reduz este número para 104, o que representa uma diminuição de aproximadamente 69%. Essa otimização permite que as equipes de segurança concentrem seus recursos de forma mais eficaz, tratando um volume menor e mais preciso de ameaças verdadeiramente prioritárias.

Para a definição do algoritmo e do número ideal de clusters (k), este trabalho apoia-se nos resultados obtidos por Silva e Souza Neto (2026). Em uma rigorosa análise comparativa prévia, os autores demonstraram, por meio do Método do Cotovelo e métricas de validação interna, que o algoritmo K-Means parametrizado com k=5 oferece o melhor equilíbrio estatístico e estrutural para a segmentação de perfis de risco em

vulnerabilidades. Dessa forma, a presente pesquisa adota diretamente essa configuração validada para investigar sua eficiência na redução operacional de alertas.

4.3.1 Perfis de risco identificados pelo k-Means

O algoritmo k-Means foi aplicado com o número de clusters definido como k=5. A análise dos centroides de cada cluster, que representam o "centro de gravidade" de cada grupo, nos permite caracterizar cinco perfis de risco distintos e acionáveis. A Tabela 1 resume as características médias de cada cluster.

Tabela 1. Caracterização dos Perfis de Risco (Centroides K-Means)

Perfil (Cluster)	EPSS Médio	NCS Médio	Interpretação Estratégica
0 - Crítico	0.33	**0.86**	Alto impacto de negócio; prioridade máxima.
1 - Alto	**0.67**	0.35	Alta probabilidade de ataque; ameaça iminente.
2 - Médio	0.34	0.41	Risco padrão; gestão contínua.
3 - Baixo	0.07	0.44	Baixa probabilidade; monitoramento.
4 - Mínimo	0.02	0.07	Risco residual; aceitável.

Fonte: Autoria própria (2026).

A Tabela 1 detalha os valores médios de EPSS e NCS para cada um dos 5 clusters. Para facilitar a interpretação e a comparação visual desses perfis. As cores mais quentes, como vermelho/laranja indicam valores mais elevados, permitindo a identificação imediata do perfil 'Crítico' como aquele que possui, simultaneamente, os maiores escores médios de probabilidade e impacto.

A seguir, uma descrição detalhada de cada perfil:

Cluster 0 - Crítico: Este perfil agrupa vulnerabilidades em sistemas de alto impacto para o negócio (NCS médio de 0.86), combinadas com uma probabilidade de exploração moderada (EPSS médio de 0.33). Embora a probabilidade de ataque não seja a mais alta, o impacto severo de uma possível exploração nesses ativos críticos torna este o grupo de maior prioridade estratégica, exigindo monitoramento constante e planejamento de correção.

Cluster 1 - Alto: Este grupo é caracterizado por vulnerabilidades com a mais alta probabilidade de exploração (EPSS médio de 0.67), porém em ativos de impacto de negócio moderado a baixo (NCS médio de 0.35). O alto volume de ataques esperado para

estas falhas as torna uma prioridade, pois representam a ameaça mais provável de se concretizar.

Cluster 2 - Médio: Este cluster representa o risco padrão, com valores médios tanto de probabilidade (EPSS médio de 0.34) quanto de impacto (NCS médio de 0.41). São as vulnerabilidades que devem ser tratadas através dos processos de gestão de vulnerabilidades contínuos da organização.

Cluster 3 - Baixo: Este perfil se destaca, pois agrupa vulnerabilidades com baixa probabilidade de exploração (EPSS médio de 0.07), mas em sistemas de impacto moderado (NCS médio de 0.44). O risco aqui é baixo, mas a criticidade do ativo exige que essas falhas não sejam ignoradas, sendo tratadas após os grupos de maior risco.

Cluster 4 - Mínimo: Este é o grupo de menor prioridade. Contém vulnerabilidades com baixa probabilidade de exploração (EPSS médio de 0.02) em sistemas de baixo impacto (NCS médio de 0.07). Representam o menor risco e podem ser abordadas após todos os demais grupos.

4.3.2 Validação com DBSCAN e análise de Outliers

A análise de densidade encontrou 5 clusters, um número consistente com nossa escolha de k=5, o que reforça a robustez da segmentação.

Para complementar a análise, foi mensurado o desempenho computacional da execução do modelo. Essa execução, do algoritmo k-Means sobre o dataset de 421 vulnerabilidades, foi concluída em aproximadamente 1 segundo. Embora este tempo seja desprezível no escopo atual, ele serve como um referencial de desempenho que reforça a viabilidade da aplicação desta metodologia em tempo real ou em datasets significativamente maiores, conforme discutido na seção de conclusão.

A aplicação do DBSCAN ao dataset resultou na identificação de cinco agrupamentos principais de alta densidade, corroborando indiretamente a escolha de k=5 feita para os métodos de particionamento. Mais importante, o DBSCAN classificou 14 pontos como 'ruído'. No contexto desta análise, esses pontos são interpretados como os outliers de interesse: vulnerabilidades com perfis de risco atípicos que não se encaixam nos agrupamentos principais e que, portanto, merecem investigação individualizada por parte das equipes de segurança.

A análise individualizada destes pontos revelou casos de risco extremo e atípico,

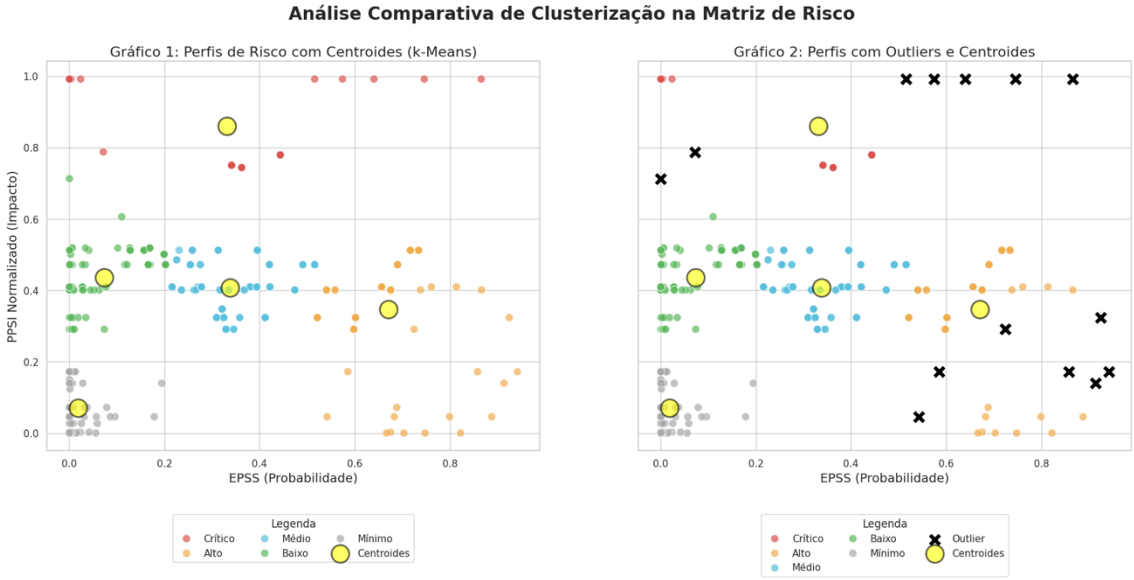
como:

a) CVE-2003-0033 (EPSS 0.52, NCS 0.99): Um ativo de impacto quase máximo com probabilidade moderada, representando uma ameaça crítica que poderia ser subpriorizada em médias simples;
b) CVE-2024-0195 (EPSS 0.92, NCS 0.32): Uma vulnerabilidade de alta probabilidade em um ativo de menor valor, servindo como um provável ponto de entrada para movimentação lateral.

4.3.3 Visualização consolidada da matriz de risco

Para consolidar os achados das análises de k-Means e DBSCAN, a Figura 4 apresenta a Matriz de Risco final. Este gráfico de dispersão mapeia cada vulnerabilidade de acordo com suas pontuações de probabilidade (EPSS) e impacto (NCS), utilizando cores para representar os cinco perfis de risco (clusters) identificados pelo k-Means e marcadores distintos para destacar os outliers apontados pelo DBSCAN.

Figura 4 – Matriz de Risco: Perfis de Risco (k-Means) e Anomalias (DBSCAN)



Fonte: Autoria própria (2026).

A visualização permite uma interpretação da segmentação do risco. Observa-se a localização distinta do cluster 'Crítico', caracterizado por altos valores de NCS. Da mesma forma, os perfis 'Baixo' e 'Mínimo' concentram-se no quadrante esquerdo, representando

parte significativa das vulnerabilidades que, embora numerosas, constituem um risco operacional menor.

Destacados com um marcador em formato de 'X', os outliers identificados pelo DBSCAN são visualmente evidentes por sua posição isolada. A existência desses pontos demonstra a capacidade da análise de densidade em capturar casos atípicos, vulnerabilidades com combinações únicas de probabilidade e impacto, que poderiam ser erroneamente agrupadas e mascaradas por modelos de particionamento baseados em centroides.

Essa matriz de risco consolidada serve como uma ferramenta de decisão estratégica. Ela não apenas categoriza a maioria das ameaças em perfis de risco objetivos, mas, também, sinaliza as anomalias que exigem uma análise humana especializada, traduzindo o resultado da análise de dados em um mapa de priorização prático e compreensível.

5 CONCLUSÃO

A gestão de vulnerabilidades em ambientes de TI é desafio, intensificado pela sobrecarga de alertas e pelas limitações na adoção de métricas de priorização unidimensionais, como o CVSS (Spring 2021). Este trabalho demonstrou que a aplicação de algoritmos de clusterização, utilizando um dataset enriquecido com métricas de probabilidade de exploração (EPSS) e impacto contextual de negócio (NCS), permite ir além de uma pontuação única de priorização, oferecendo uma compreensão mais adequada do cenário de risco.

A principal contribuição deste trabalho foi a revelação de que as vulnerabilidades não se comportam como uma massa homogênea, mas se agrupam em perfis de risco distintos e acionáveis, ou seja, perfis que permitem a associação direta a estratégias e ações de tratamento específicas e priorizadas (como remediação imediata, monitoramento ou aceitação do risco). Em contraste com abordagens que geram uma pontuação numérica única, a clusterização segmenta o cenário de ameaças em perfis qualitativos distintos. A segmentação em clusters fornece aos gestores de segurança uma visão estratégica. Essa abordagem permite a alocação de recursos de forma eficiente, aplicando estratégias de remediação, monitoramento ou aceitação de risco, que são específicas para a natureza de cada perfil, ao invés de uma abordagem única para todas as falhas.

Como trabalhos futuros, este trabalho abre diversas possibilidades. Primeiramente, a metodologia pode ser expandida com a inclusão de novas características, como dados de Inteligência de Ameaças em tempo real, uma abordagem que já demonstrou valor na literatura para enriquecer modelos de risco (Rodriguez, 2020; Okamura, 2020). Além disso, a aplicação de algoritmos, como ensembles de clusterização, poderia ser explorada. No entanto, é importante ressaltar que tais pesquisas devem avaliar não apenas a qualidade do agrupamento, mas também a complexidade computacional e a escalabilidade. Qualquer ganho na robustez do agrupamento deve ser ponderado em relação à complexidade computacional do k-Means. Conforme aponta a literatura, algoritmos como o k-Means possuem baixa complexidade computacional, o que garante sua viabilidade para aplicação em larga escala, em contraste com métodos de maior complexidade (Saxena *et al*., 2017). Portanto, a escolha de algoritmos alternativos deve considerar o potencial aumento no custo computacional. Por fim, uma evolução natural deste trabalho é o uso de modelos supervisionados, como Random Forest ou XGBoost, onde os perfis de risco aqui identificados seriam usados como rótulos para treinar um modelo capaz de automatizar a classificação de novas vulnerabilidades, uma técnica explorada em outros trabalhos (Althar *et al*., 2022).

Entretanto, é preciso reconhecer as limitações deste estudo. A principal delas reside na geração das pontuações NCS: embora baseada em um framework estruturado e em uma hipótese que correlaciona a contagem de vulnerabilidades à importância dos sistemas, a avaliação de criticidade resulta de um modelo, e não reflete uma coleta de dados de campo com os gestores de cada ativo. Adicionalmente, o dataset de vulnerabilidades, embora derivado de um relatório de varredura real, passou por processos de balanceamento e enriquecimento sintético, e a amostra de ativos pertence a uma única organização. Esses fatores indicam que os perfis de risco encontrados são representativos do cenário modelado, mas sua generalização para outras organizações requer atenção.

Além disso, sugere-se a revisão e reaplicação da metodologia apresentada à medida que novas atualizações do PPSI ou das Normas Complementares (NCS) do GSI, como a possível formalização de métricas para identificação de ativos críticos, sejam oficialmente publicadas.

Este trabalho mostra que a aplicação da ciência de dados, especificamente a clusterização, transforma a gestão de vulnerabilidades de uma tarefa reativa e baseada em

volume para um processo proativo, ágil e estratégico, focado no risco real e contextualizado ao negócio.

REFERÊNCIAS

AL MAMUN, A. *et al.,* Machine learning for stock market security measurement: a comparative analysis of supervised, unsupervised, and deep learning models. **The American Journal of Engineering and Technology**, v. 6, n. 11, p. 63-76, 2024.

ALTHAR, R. R. *et al.,* Automated risk management based software security vulnerabilities management. **IEEE Access**, v. 10, p. 90597-90608, 2022.

CVEDETAILS. **CVEdetails - Vulnerability Statistics**. 2025. Disponível em: https://www.cvedetails.com/.

ESTER, M. *et al.,* A density-based algorithm for discovering clusters in large spatial databases with noise. In: INTERNATIONAL CONFERENCE ON KNOWLEDGE DISCOVERY AND DATA MINING (KDD'96), 2., 1996. **Proceedings [...]**. [S.l.: s.n.], 1996. p. 226-231.

FIRST.ORG, INC. **Common Vulnerability Scoring System v3.1: Specification Document**. 2019. Disponível em: https://www.first.org/cvss/v3-1/specification-document.

FIRST.ORG, INC. **Exploit Prediction Scoring System (EPSS) User Guide**. 2024. Disponível em: https://www.first.org/epss/user-guide.

FUHNWI, G. S. *et al.,* An empirical study on anomaly detection using density-based and representative-based clustering algorithms. **Journal of the Nigerian Society of Physical Sciences**, v. 5, p. 1364, 2023.

GIL, A. C. **Como elaborar projetos de pesquisa**. 4. ed. [S.l.]: Atlas, 2002.

GOSWAMI, M. J. AI-Based Anomaly Detection for Real-Time Cybersecurity. **International Journal of Research and Review Techniques (IJRRT)**, v. 3, n. 1, p. 45-53, 2024.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 27005:2022 - Information security, cybersecurity and privacy protection — Guidance on managing information security risks**. 2022.

JACOBS, J. *et al.,* Enhancing vulnerability prioritization: Data-driven exploit predictions with community-driven insights. In: IEEE EUROPEAN SYMPOSIUM ON SECURITY AND PRIVACY WORKSHOPS (EuroS&PW), 2023. **Proceedings [...]**. [S.l.]: IEEE, 2023. p. 194-206.

JAMES, G. *et al.,* **An Introduction to Statistical Learning**: Applications in R. 2. ed. [S.l.]: Springer, 2021.

LAKATOS, E. M.; MARCONI, M. de A. **Fundamentos de metodologia científica**. 8. ed. [S.l.]: Atlas, 2017.

MACQUEEN, J. B. Some methods for classification and analysis of multivariate observations. In: BERKELEY SYMPOSIUM ON MATHEMATICAL STATISTICS AND PROBABILITY, 5., 1967. **Proceedings [...]**. [S.l.: s.n.], 1967. v. 1, p. 281-297.

MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS (MGI). **Framework do PPSI - Guia**. 2024. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_framework_psi.pdf.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **NVD - CVE Metrics**. 2024. Disponível em: https://nvd.nist.gov/vuln/reporting/nvd-dashboard.

PANT, Y. R.; LEIGH, L.; RUEDA, J. F. Improving k-means clustering: a comparative study of parallelized version of modified k-means algorithm for clustering of satellite images. **Algorithms**, v. 18, n. 8, p. 532, 2025.

PRODANOV, C.; FREITAS, E. C. **Metodologia do trabalho científico**: métodos e técnicas da pesquisa e do trabalho acadêmico. 2. ed. Novo Hamburgo: Editora Feevale, 2013.

QUALYS, INC. **Qualys Web Application Scanning (WAS)**. 2025. Disponível em: https://www.qualys.com/apps/web-app-scanning/. Acesso em: 08 out. 2025.

RODRIGUEZ, A.; OKAMURA, K. Enhancing data quality in real-time threat intelligence systems using machine learning. **Social Network Analysis and Mining**, v. 10, n. 1, p. 91, 2020.

SAXENA, A. *et al.*, A review of clustering techniques and developments. **Neurocomputing**, v. 267, p. 664-681, 2017.

SILVA, M. L. M. da; SOUZA NETO, J. Uma análise comparativa de algoritmos de clusterização para a definição de perfis de risco de vulnerabilidades. **Revista Delos**, v. 19, n. 79, p. e9206, 2026. DOI: 10.55905/rdelosv19.n79-066.

SPRING, J. M. **Prioritizing Vulnerability Response**: A Stakeholder-Specific Vulnerability Categorization. [S.l.]: Carnegie Mellon University, Software Engineering Institute, 2021.

TENABLE, INC. **Tenable Vulnerability Management**. 2025. Disponível em: https://www.tenable.com/products/tenable-io. Acesso em: 08 out. 2025.

TRIBUNAL DE CONTAS DA UNIÃO (TCU). **Acórdão 1.889/2020-TCU-Plenário**. 2020.

TUKEY, J. W. **Exploratory Data Analysis**. [S.l.]: Addison-Wesley, 1977.

VAL, O. O. *et al.*, Strengthening cybersecurity measures for the defense of critical infrastructure in the United States. **SSRN Electronic Journal**, 2025.