**CENTRO PAULA SOUZA**
**FACULDADE DE TECNOLOGIA DE ARARAQUARA**
**CURSO DE GRADUAÇÃO EM SEGURANÇA DA INFORMAÇÃO**

**Micaele Oliveira da Silva**

# SEGURANÇA DA INFORMAÇÃO NO MONITORAMENTO EM REDES DE COMPUTADORES

Orientador: Prof. André Castro Rizo

Araraquara
**2º semestre/2024**

## AGRADECIMENTOS

Agradeço a Deus por me dar forças para superar os desafios desta jornada de três anos de aprendizado e dedicação. Aos meus pais, Ednéia Silva da Silva e Elisvaldo Oliveira Silva, sou imensamente grata pelo amor, apoio e ensinamentos que me guiaram até aqui, assim como à minha família e amigos, que sempre me incentivaram com carinho.

Meu especial reconhecimento ao meu companheiro, Gabriel Henrique de Jesus Silva, por seu amor, paciência e suporte constante. Manifesto minha profunda gratidão ao meu orientador, André Castro Rizo, cujas orientações, comprometimento e exemplo profissional foram fundamentais para o sucesso deste trabalho. Também agradeço ao professor Wdson de Oliveira, cuja atenção, cuidado e ensinamentos enriqueceram meu aprendizado e me ajudaram a superar os desafios com confiança e determinação.

Sou igualmente grata aos colegas de trabalho, que estiveram presentes ao longo do caminho, contribuindo com trocas de conhecimento e apoio mútuo. Cada colaboração foi essencial na construção deste trabalho.

Por fim, agradeço aos professores da instituição, que contribuíram não apenas para minha formação acadêmica, mas também para meu crescimento pessoal. A todos que fizeram parte dessa conquista, meu mais sincero obrigado.

## SUMÁRIO

## RESUMO

Este estudo aborda a segurança da informação aplicada ao monitoramento de redes de computadores com foco nos pilares de confidencialidade, integridade e disponibilidade, destacando a importância do monitoramento contínuo como estratégia central para identificar e mitigar ameaças, onde práticas bem estruturadas de segurança podem prevenir incidentes graves e manter a confiabilidade das operações, enquanto a conformidade com normas internacionais é apresentada como essencial para a implementação de processos seguros e eficazes, reforçando a gestão de riscos e políticas de segurança adaptáveis que fortalecem a proteção das redes contra vulnerabilidades, o que evidencia a relevância de estratégias baseadas em padrões consistentes que englobam desde a detecção precoce de anomalias até a mitigação de impactos, integrando processos, políticas e equipes treinadas para enfrentar um cenário de ameaças cibernéticas em constante evolução, consolidando o monitoramento como um elemento essencial na manutenção da segurança e continuidade das operações digitais.



Palavras-chave: Segurança da informação; monitoramento de redes; monitoramento contínuo; confidencialidade; integridade; disponibilidade; gestão de riscos; políticas de segurança; detecção de anomalias; estratégias de cibersegurança.



## ABSTRACT

This study addresses information security applied to network monitoring, focusing on the pillars of confidentiality, integrity, and availability, highlighting the importance of continuous monitoring as a central strategy to identify and mitigate threats, where well-structured security practices can prevent severe incidents and maintain operational reliability, while compliance with international standards is presented as essential for implementing secure and effective processes, reinforcing risk management and adaptable security policies that strengthen network protection against vulnerabilities, which highlights the relevance of strategies based on consistent standards that encompass everything from early anomaly detection to impact mitigation, integrating processes, policies, and trained teams to face an ever-evolving cyber threat landscape, consolidating monitoring as an essential element in maintaining security and continuity of digital operations.



Keywords: Information security; network monitoring; continuous monitoring; confidentiality; integrity; availability; risk management; security policies; anomaly detection; cybersecurity strategies.

## 1. INTRODUÇÃO

Em um mundo cada vez mais interconectado, onde bilhões de dispositivos dependem de redes de computadores para a troca de dados e o acesso à internet, a segurança da informação emerge como um elemento crítico para a proteção das infraestruturas digitais.

A necessidade de proteger as redes de computadores da crescente exponencial de anomalias no meio digital exige assim um monitoramento contínuo e sofisticado, essencial para manter a confidencialidade, integridade e disponibilidade dos dados.

Conforme destacado por Hintzbergen et al. (2018, p. 20) a segurança da informação é alcançada através da implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Esses controles precisam ser estabelecidos, implementados, monitorados, revisados e melhorados, onde necessário, para assegurar que os objetivos específicos de segurança e do negócio da organização sejam atendidos.

No contexto dos computadores, a segurança de redes emerge como um dos pilares fundamentais, operando como um componente essencial no escopo da segurança da informação com enfoque exclusivo na proteção da informação trafegada entre indivíduos e sistemas presentes no ambiente digital, onde busca garantir que os dados que transitam pelas redes estejam protegidos.

As redes de computadores, ao interligarem dispositivos dos usuários a uma vasta gama de recursos e informações digitais, criam um sistema robusto de conexões que viabilizam a comunicação e o compartilhamento de dados entre cada ponto na rede.

Conforme menciona Tanenbaum (1996), as redes de computadores como um número grande de computadores independentes, porém interligados, que realizam as tarefas de alguma instituição. Ainda segundo o autor, dois computadores estão interligados se eles são capazes de trocar informações.

Diante desse cenário, o monitoramento em redes de computadores consolida-se com uma posição indispensável, desempenhando um papel estratégico na identificação, antecipação e resposta a anomalias e atividades suspeitas que possam comprometer a segurança da rede.

Como destaca Sousa (2013) uma boa infraestrutura de rede de computadores possibilita que empresas vendam mais, produzam mais e gerem mais empregos. Dentro das empresas, as tecnologias e equipamentos estão em constante evolução, sempre em busca da

maior qualidade e menor índice de falhas, visando trazer ao usuário mais tranquilidade ao utilizar os equipamentos.

Desta forma, o monitoramento vai além da mera detecção de comportamentos inadequados e a implementação de ações preventivas que garantam a integridade e a disponibilidade dos serviços, trazendo à tona a crucialidade em um ambiente onde o tráfego cresce exponencialmente, multiplicando os desafios e exigindo soluções proativas e eficazes no combate aos riscos às redes de computadores para assegurar sua integridade, autenticidade e disponibilidade.

Conforme destacado por Hintzbergen et al. (2018, p. 20), a segurança da informação é importante tanto para os negócios públicos quanto para o setor privado, sendo crucial para a proteção de infraestruturas críticas.

Neste sentido, este trabalho propõe analisar as implicações da segurança da informação no monitoramento em redes de computadores, abordando como os pilares fundamentais da segurança da informação podem ser aplicados no contexto de proteção da informação em redes digitais que interligam os sistemas computacionais. Visa, ainda, enaltecer práticas que impactam a vigilância em ecossistemas digitais de computadores, com o objetivo de fornecer uma visão detalhada sobre como essa interação entre tecnologias de controle seguras pode gerar redes confiáveis e robustas, permitindo a prevenção de anomalias de segurança.

## 2. REFERÊNCIAL TEÓRICO

O posicionamento estratégico vigente pela segurança da informação nas redes de computadores consiste em uma aplicação estruturada de práticas e princípios que garantem a proteção dos dados ao longo de todo o seu ciclo de vida, sustentado pelos pilares da confidencialidade, integridade e disponibilidade, a observação dos sistemas interligados promove uma abordagem que visa à proteção do armazenamento, da utilização e da transferência de informações pelas estruturas de comunicação, assegurando redes robustas e resilientes contra anormalidades cibernéticas.

Conforme destacado por Leinwand e Conroy (1996), a gestão eficaz de redes é fundamental para manter a integridade, confidencialidade e disponibilidade dos dados. Eles enfatizam que o monitoramento contínuo permite a detecção precoce de anomalias e a implementação de medidas corretivas, assegurando que os recursos de rede estejam sempre

disponíveis e protegidos contra acessos não autorizados.

Além disso, Leinwand e Conroy (1996) discutem a importância de políticas de segurança robustas que integrem controles de acesso rigorosos e mecanismos de autenticação. Eles argumentam que tais medidas são essenciais para prevenir alterações não autorizadas e garantir a precisão dos dados, alinhando-se aos pilares fundamentais da segurança da informação.

Conforme destacado por Comer (2016), o monitoramento de redes é essencial para garantir a qualidade do serviço, permitindo o provisionamento adequado e a manutenção da estabilidade e eficiência da operação da rede. Além disso, Basso (2020) enfatiza que o monitoramento contínuo das atividades de rede é fundamental para detectar anomalias e prevenir ameaças, assegurando a integridade e a disponibilidade dos dados e recursos.

Destacando assim que o acesso seguro à informação em redes de computadores baseia-se em princípios que asseguram a proteção da comunicação digital entre máquinas, orientando políticas e controles voltados para a gestão segura dos dados e a continuidade dos sistemas, promovendo a coesão e o controle em um ambiente cibernético estruturado.

## 2.1 Princípios fundamentais da segurança da informação em redes de computadores

Em um contexto orientado a computadores, os princípios de segurança da informação são divididos em três objetivos, cujo cerne é a informação e sua acessível permanência, permitindo que indivíduos ou sistemas que detém autorização façam o acesso a ela, assim, buscando manter a privacidade à informação e garantindo de maneira precisa a integridade dos dados, evitando alterações que comprometam a consistência e a disponibilidade das infraestruturas para que operações essenciais atuem sem interrupções.

Conforme esclarece por NIST[1]:

> *"A segurança da informação não é um processo estático e requer monitoramento e gerenciamento contínuos para proteger a confidencialidade, integridade e disponibilidade das informações, bem como para garantir que novas vulnerabilidades e ameaças em evolução sejam rapidamente identificadas e tratadas de forma adequada. Diante de uma força de trabalho e de um ambiente tecnológico em constante evolução, é essencial que as organizações forneçam informações precisas e oportunas, enquanto operam em um nível de risco aceitável.".*

[1] NIST SP 800-12 Rev. 1, 2017, p. 10, tradução nossa

Esses fundamentos ganham a máxima importância na estrutura das redes de computadores, pois a própria estrutura da interconexão entre sistemas digitais permite o fluxo de informações e o compartilhamento de recursos entre dispositivos em configurações locais e globais, onde menciona TANENBAUM at al.: "Como as redes frequentemente diferem em aspectos importantes, transferir pacotes de uma rede para outra nem sempre é fácil. Devemos abordar problemas de heterogeneidade e também problemas de escala à medida que a internet resultante cresce muito." (TANENBAUM; WETHERALL, 2011, p. 425, tradução nossa).

Também esclarecido por TANENBAUM[2]:

> *"Os problemas de segurança de rede podem ser divididos aproximadamente em quatro áreas intimamente interligadas: sigilo, autenticação, não repúdio e controle de integridade. O sigilo, também chamado de confidencialidade, está relacionado a manter as informações longe das mãos imundas de usuários não autorizados. É isso que geralmente vem à mente quando se pensa em segurança de rede.".*

Assim, as redes de computadores são compostas por uma combinação de tecnologias e protocolos que permitem a comunicação entre servidores, estações de trabalho e dispositivos móveis de forma eficiente e segura.

Nesta perspetiva, devido ao papel crítico que a rede de computadores desempenha na comunicação digital, a segurança da informação e de redes emerge para garantir que todo o tráfego de dados presente na infraestrutura contenha seus princípios por meio de uma a implementação de práticas de monitoramento contínuo que visa a aplicação de seus pilares. Com base no entendimento de Kurose, destaca que "À medida que a Internet pública e as intranets privadas evoluíram de pequenas redes para uma grande infraestrutura global, a necessidade de gerenciar o enorme número de componentes de hardware e software dentro dessas redes de forma mais sistemática tornou-se mais importante." (KUROSE; ROSS, 2013, p. 756, tradução nossa).

Pelo exposto, os princípios fundamentais da segurança da informação, como a confidencialidade que protege o acesso a dados sensíveis, a integridade que garante que as informações não sejam alteradas de forma indevida e a disponibilidade que assegura acesso contínuo mesmo diante de falhas, são essenciais para a operação segura das redes de computadores, onde esses pilares, quando integrados a práticas eficazes de monitoramento contínuo e gerenciamento eficiente de recursos, formam a base para enfrentar ameaças em

[2] TANENBAUM; WETHERALL, 2011, p. 764, tradução nossa

constante evolução nas infraestruturas digitais.

## 2.2 Zabbix e o monitoramento de redes de computadores

No contexto de redes de computadores, o monitoramento com o Zabbix revela-se uma opção atrativa, pois oferece resultados claros e eficientes, garantindo a integridade dos dados coletados e proporcionando percepções em tempo real.

Conforme mencionado na documentação oficial da empresa Zabbix[3], é esclarecido que a plataforma utiliza mecanismos projetados para permitir uma resposta ágil a incidentes que possam comprometer a integridade dos dados:

> *"O Zabbix é uma solução de nível enterprise, de código aberto e com suporte a monitoração distribuída. O Zabbix é um software que monitora numerosos parâmetros de rede, a saúde e integridade de servidores, máquinas virtuais, aplicações, serviços, banco de dados, websites, a nuvem e muito mais. O Zabbix usa um mecanismo flexível de notificação que permite aos usuários configurar alertas baseados em e-mail para praticamente qualquer evento. Isso permite uma resposta rápida para problemas do servidor. O Zabbix oferece um excelente recurso de relatórios e visualização de dados baseados em dados armazenados. Isso torna o Zabbix ideal para gerenciamento de capacidade."*

## 2.3 A relevância do monitoramento na segurança das redes

Em termos de segurança da informação, o monitoramento vai além de observar o tráfego de dados e as atividades gerais do sistema, funcionando como uma medida preventiva que protege e assegura a funcionalidade ideal das redes de computadores. Este entendimento se estende pela compreensão mencionada por Saydam[4] at al., conforme destaca:

> *"A gestão de redes inclui a implantação, integração e coordenação dos elementos de hardware, software e humanos para monitorar, testar, pesquisar, configurar, analisar, avaliar e controlar os recursos da rede e dos elementos para atender aos requisitos de desempenho operacional em tempo real e de Qualidade de Serviço a um custo razoável."*

Associado aos princípios de segurança, ele promove uma infraestrutura digital confiável e capaz de responder rapidamente às demandas de um ambiente interconectado e em constante evolução.

Conforme destaca NIELES[5] et al.:

[3] Zabbix, 2024, p. 7.
[4] SAYDAM; MAGEDANZ, 1996, p. 345, tradução nossa.
[5] NIELES; DEMPSEY; PILLITTERI, 2017, p. 64, tradução nossa

> "*Embora as ameaças que hackers e códigos maliciosos representam para sistemas e redes sejam bem conhecidas, a ocorrência de tais eventos prejudiciais continua sendo imprevisível. Incidentes de segurança em redes maiores (por exemplo, a Internet), como invasões e interrupções de serviço, prejudicaram as capacidades computacionais de várias organizações. Quando inicialmente confrontadas com esses incidentes, a maioria das organizações responde de maneira para isso. No entanto, a recorrência de incidentes semelhantes pode tornar custo-beneficial desenvolver uma capacidade padrão para descoberta rápida e resposta a tais eventos.".*

Destaca-se que o monitoramento não se limita a proteger a rede contra eventos adversos, mas também atua preventivamente, envolvendo uma análise avançada de tráfego e comportamento para identificar e mitigar potenciais vulnerabilidades antes que impactem negativamente as operações de tráfego digital.

Em um cenário de redes cada vez mais complexas que incorporam dispositivos ponta-a-ponta e ambientes híbridos, o acompanhamento contínuo se torna indispensável para acompanhar o crescimento da interconexão entre dispositivos e o ritmo acelerado das mudanças tecnológicas. Conforme destaca KOSTOPOULOS[6]:

> *"O aumento da velocidade das redes, combinado com o igualmente crescente tamanho da memória e do armazenamento dos computadores, agora permite a incorporação de algoritmos avançados nos nós da rede, onde o tráfego pode ser monitorado, avaliado e controlado.".*

O monitoramento contínuo consolida-se como um elemento crítico para garantir a segurança e a resiliência operacional da rede, pois, além de proteger a rede, ele assegura que os princípios da segurança da informação sejam aplicados de maneira consistente, garantindo que os dados permaneçam íntegros e que a rede esteja disponível para as operações essenciais e protegida contra riscos de segurança. Destacado por KOSTOPOULOS em: "Como sistema, os eles da Internet são um recurso subutilizado. Uma vez que inteligência relacionada à segurança seja inserida neles, um ecossistema de defesa cibernética será criado." (KOSTOPOULOS, 2017, p. 191, tradução nossa).

[6] KOSTOPOULOS, 2017, p. 189, tradução nossa.

## 3. METODOLOGIA

Com o intuito de contextualizar o tema do artigo em questão, foi desenvolvida uma pesquisa qualitativa, permitindo identificar padrões, boas práticas e lacunas nos processos existentes e ser facilmente replicável em organizações similares, com caráter exploratório e descritivo, conduzida por meio de um estudo de caso com o objetivo de analisar as práticas de uma empresa do setor de monitoramento de redes de computadores e verificar o alinhamento dessas práticas aos princípios fundamentais da segurança da informação, apresentando uma visão detalhada sobre as operações de segurança essenciais no monitoramento de redes.

O estudo foi realizado na sede de uma empresa do ramo de Tecnologia da Informação especializada em monitoramento de ambientes de TI, fornecendo um ambiente propício para as investigações sobre segurança da informação devido à sua infraestrutura tecnológica robusta e à atuação direta em operações críticas de monitoramento, proporcionando um modelo confiável para estudos futuros e permitindo a execução da pesquisa foi organizada em etapas bem definidas, com foco na coleta de dados qualitativos por meio de uma análise documental abrangente, que incluiu políticas internas, relatórios técnicos, registros de auditoria e outros documentos que refletem as práticas de segurança e conformidade organizacional para garantir uma análise robusta, assegurando representatividade e profundidade na avaliação das práticas de segurança da informação da organização.

A análise aprofundada oferece, portanto, uma base sólida para o entendimento de estratégias destinadas a aumentar a eficiência, a resiliência e a segurança das operações em redes de computadores organizacionais.

### 3.1 Infraestrutura digital confiável com ferramentas de monitoramento aplicadas a rede

Para construir uma infraestrutura digital confiável, é necessário implementar ferramentas de monitoramento contínuo que garantam a supervisão do tráfego de dados e das atividades do sistema, permitindo a detecção precoce de anomalias e a estabilidade da rede; para isso, é fundamental identificar as necessidades específicas de monitoramento, definir métricas relevantes e instalar as ferramentas em pontos estratégicos, complementando com alertas automatizados para eventos críticos e painéis que possibilitem o acompanhamento em tempo real e a análise proativa de tendências, enquanto soluções como o Zabbix podem centralizar e fortalecer o gerenciamento, assegurando uma infraestrutura resiliente e preparada para desafios.

Conforme destacado STALLINGS[7] at al:

> *"Idealmente, você também deve ter alguma forma de monitoramento automatizado de rede e sistema de detecção de intrusões em execução, para que o pessoal seja notificado caso tráfego anormal seja detectado. [...] É importante que uma organização conheça seus padrões normais de tráfego, para que tenha uma linha de base com a qual possa comparar fluxos de tráfego anormais.".*

Ferramentas como o Zabbix oferecem recursos robustos para o monitoramento de redes, permitindo a coleta de dados em tempo real e a análise de desempenho dos componentes da rede. Conforme menciona ZABBIX a empresa: “O Zabbix é um software que monitora numerosos parâmetros de rede, a saúde e integridade de servidores, máquinas virtuais, aplicações, serviços, banco de dados, websites, a nuvem e muito mais.” (ZABBIX, 2024, p. 7).

Esclarecendo que a ferramenta possibilita o acompanhamento contínuo dos recursos de rede, identificando rapidamente falhas e garantindo a disponibilidade dos serviços por meio de uma configuração de alertas personalizados e a geração de relatórios detalhados sobre anomalias da rede, onde seu modus operandi se integram nese sentido, a integração de sistemas de detecção e prevenção de intrusões (IDPS), onde fortalece a segurança da rede, monitorando atividades suspeitas e bloqueando ameaças em tempo real.

Conforme esclarece KOSTOPOULOS[8]:

> *"Tais sistemas, compostos por hardware e/ou software, são chamados de Sistemas de Detecção e Prevenção de Intrusões (IDPS, frequentemente pronunciado como 'eye-deps'). Dependendo da aplicação específica, um sistema pode ser um IDS, ou seja, apenas um Sistema de Detecção de Intrusões, sem capacidades de prevenção, ou pode ser um IDPS, às vezes ainda chamado de IDS, que possui ambas as capacidades: detecção e prevenção.".*

Evidenciando assim que a adoção de ferramentas de monitoramento automatizado não apenas fortalece a segurança das redes de computadores, mas também assegura a aplicação consistente dos princípios fundamentais da segurança da informação, garantindo a integridade, confidencialidade e disponibilidade dos dados e serviços.

## 3.2 Os centros de operações no monitoramento seguro de redes

A centralização e controles de segurança em redes de computadores é um tópico

[7] STALLINGS; BROWN, 2015, p. 263, tradução nossa.
[8] KOSTOPOULOS, 2017, p. 109, tradução nossa.

crucial, exigindo equipes especializadas e capacitações específicas para garantir a proteção dos dados e a continuidade das operações.

Conforme esclarece ZIMMERMAN[9] em:

> *"O centro de operações de segurança cibernética (CSOC) de hoje deve ter tudo o que precisa para montar uma defesa competente da sempre mutável infraestrutura de tecnologia da informação (TI). Isso inclui uma vasta gama de tecnologias sofisticadas de detecção e prevenção, um mar virtual de relatórios de inteligência cibernética e acesso a uma força de trabalho em rápida expansão de profissionais de TI talentosos.".*

Destaca-se como os Centros de Operações de Segurança (SOC - Security Operation Center) e os Centros de Operações de Rede (NOC - Network Operation Center) desempenham papéis complementares e indispensáveis nesse cenário, operando de forma coordenada para assegurar tanto a conformidade da segurança da informação quanto a estabilidade da infraestrutura. Pois, segundo Zimmerman destaca "Uma série de tecnologias permite que o SOC examine milhões de eventos todos os dias, apoiando o ciclo de vida dos incidentes desde o início até a conclusão." (ZIMMERMAN, 2014, p. 12, tradução nossa) e reitera afirmando "Um SOC é uma equipe composta principalmente por analistas de segurança, organizada para detectar, analisar, responder, relatar e prevenir incidentes de segurança cibernética." (ZIMMERMAN, 2014, p. 9, tradução nossa).

Ainda que, de acordo com Zimmerman, "Um *SOC* é distinto de um *NOC* porque o SOC está primordialmente focado em buscar ataques cibernéticos, enquanto o *NOC* está preocupado com a operação e manutenção dos equipamentos de rede." (ZIMMERMAN, 2014, p. 13, tradução nossa), onde enaltece as resoluções em que ambos desempenham funções críticas, mesmo que com objetivos distintos para com sua operação contínua de gestão e manutenção da infraestrutura de rede, onde complementa Zimmerman esclarecendo: "Para apoiar uma comunidade saudável, as funções do *NOC* e do *SOC* devem ser vistas como parceiros iguais, e não como uma subordinada à outra." (ZIMMERMAN, 2014, p. 78, tradução nossa).

Essa integração entre *NOC* e *SOC* abre caminho para um fluxo operacional alinhado, onde o *NOC* garante a estabilidade e a performance operacional da rede e o *SOC* concentra-se na análise e mitigação de ameaças de segurança, criando uma abordagem

[9] ZIMMERMAN, 2014, p. 1, tradução nossa.

integrada de monitoramento que reforça a resiliência da rede com uma abordagem que vida ajustes em configurações e implementação de soluções preventivas. Em que reforça Zimmerman em "Fomentar relacionamentos fortes ajuda um *SOC* a executar sua missão, especialmente quando pode haver falta de autoridade ou recursos." (ZIMMERMAN, 2014, p. 281, tradução nossa), destacando sua imponência mediante a segurança da infraestrutura de redes de computadores.

### 3.3 Normas de segurança em processos de monitoramento seguro de redes

No contexto do monitoramento de redes de computadores, a aplicação de normas internacionais, como a *ISO/IEC 27001* e a *ISO/IEC 27002*, é fundamental para garantir a conformidade com as melhores práticas de segurança da informação.

Conforme destaca a *ISO/IEC 27001:2022*:

> *"O sistema de gestão de segurança da informação preserva a confidencialidade, a integridade e a disponibilidade das informações por meio da aplicação de um processo de gestão de riscos e transmite confiança às partes interessadas de que os riscos estão sendo gerenciados adequadamente."*

A norma *ISO/IEC 27001* fornece uma abordagem sistemática para a proteção de informações críticas, estabelecendo os requisitos para a implementação de um Sistema de Gestão de Segurança da Informação (SGSI).

Esta norma oferece uma estrutura clara para o gerenciamento de riscos e a proteção da informação, possibilitando que as organizações implementem controles robustos para mitigar riscos, assegurando que os processos de monitoramento sejam realizados de forma consistente com os objetivos organizacionais e as políticas de segurança globais.

Por outro lado, a *ISO/IEC 27002* oferece diretrizes mais detalhadas, focando em controles de segurança práticos. Conforme destaca a *ISO/IEC 27002:2022*, "A segurança da informação é alcançada pela implementação de um conjunto adequado de controles, incluindo políticas, regras, processos, procedimentos, estruturas organizacionais e funções de software e hardware." (*ISO/IEC 27002:2022*, p. vii, tradução nossa), onde visa orientar as organizações sobre como aplicar controles específicos para monitoramento contínuo, visando identificar e mitigar riscos antes que se transformem em ameaças reais.

Esses controles incluem artifícios necessários para o monitoramento contínuo das redes e orientações para implementar medidas que detectem e respondam a ameaças em tempo

real, garantindo que os sistemas permaneçam protegidos contra acessos não autorizados e falhas operacionais.

O monitoramento contínuo é um elemento essencial para a defesa das redes, pois permite uma vigilância constante e a mitigação de riscos antes que se tornem ameaças reais para a segurança da informação. Conforme destaca a *ISO/IEC 27001:2022*, ""As configurações, incluindo configurações de segurança, de hardware, software, serviços e redes devem ser estabelecidas, documentadas, implementadas, monitoradas e revisadas." (*ISO/IEC 27001:2022*, p. 16, tradução nossa), onde reitera ainda a *ISO/IEC 27002:2022*, "Redes, sistemas e aplicações devem ser monitorados em busca de comportamentos anômalos, e ações apropriadas devem ser tomadas para avaliar potenciais incidentes de segurança da informação." (*ISO/IEC 27001:2022*, p. 16, tradução nossa), contribuindo diretamente para a continuidade dos negócios e compreensão de medidas de proteção para com as estruturas de computação em redes.

Essas normas estabelecem as bases para um monitoramento eficaz das redes de computadores, assegurando que sejam protegidas e que suas operações sejam mantidas sem interrupções, onde esclarece *ISO/IEC 27001:2022*, "A gestão deve demonstrar apoio à política de segurança da informação, às políticas específicas por tópico, aos procedimentos e aos controles de segurança da informação." (*ISO/IEC 27001:2022*, p. 13, tradução nossa).

Enaltece a *ISO/IEC 27001:2022*[10]:

> *"As regras de controle de acesso também podem conter elementos dinâmicos (por exemplo, uma função que avalia acessos anteriores ou valores específicos do ambiente). As regras de controle de acesso podem ser implementadas com diferentes níveis de granularidade, abrangendo desde redes ou sistemas inteiros até campos de dados específicos, e podem também considerar propriedades como a localização do usuário ou o tipo de conexão de rede utilizada para o acesso. Esses princípios e como a granularidade do controle de acesso é definida podem ter um impacto significativo nos custos. Regras mais rigorosas e maior granularidade geralmente levam a custos mais elevados. Os requisitos de negócios e as considerações de risco devem ser utilizados para definir quais regras de controle de acesso serão aplicadas e qual nível de granularidade será necessário."*

Assim, os controles de segurança aplicados de maneira sistemática e alinhados às regulamentações e melhores práticas globais tornam o monitoramento um processo essencial e estruturado, contribuindo para a resiliência e a segurança das redes, alinhado aos objetivos estratégicos da organização.

[10] ISO/IEC 27001:2022, p. 28, tradução nossa.

## 4. APLICAÇÃO, ANÁLISE DOS RESULTADOS E DISCUSSÃO

A análise interpretará como o monitoramento contínuo se alinha com os principais princípios de segurança da informação, enfatizando as interações entre as práticas implementadas e os desafios encontrados na proteção de redes de computadores.

O estudo de caso realizado centrou-se em um incidente específico enfrentado por uma empresa do setor de monitoramento de redes de computadores. A empresa identificou uma atividade anômala em seus sistemas, causada pelo *malware Perfctl*, projetado para operar de forma persistente e furtiva utilizando *rootkits*. Esse *malware* foi detectado durante a análise de um padrão incomum de uso constante de CPU nos servidores, comportamento que só cessava quando acessado via SSH. A resposta rápida a essa ameaça demonstrou a eficácia das ferramentas de monitoramento contínuo, como o Zabbix, e das práticas de segurança implementadas. Este caso fornece uma perspectiva prática sobre como tecnologias avançadas e estratégias proativas podem mitigar riscos cibernéticos e proteger infraestruturas críticas.

### 4.1 Conformidade com as normas *ISO/IEC*

Este tópico examina como as práticas e ferramentas utilizadas pela empresa analisada foram alinhadas às normas *ISO/IEC 27001* e *27002*, destacando a relevância de um sistema de monitoramento contínuo na proteção contra incidentes de segurança, como o enfrentado no caso estudado. O objetivo é demonstrar como a conformidade com essas normas contribuiu para a detecção e mitigação da ameaça, fortalecendo a postura da organização frente a riscos cibernéticos.

De acordo com o caso analisado, a empresa apresenta uma postura que reflete uma gestão robusta e adequada às exigências normativas aplicáveis no contexto dos projetos gerenciados, onde as políticas e as normas serão estabelecidas no princípio dos projetos, assegurando a conformidade com os tipos de tratamento aplicados aos dados, sempre com o objetivo de garantir que os serviços fornecidos estejam alinhados às melhores práticas de segurança da informação e com as normas da *ISO*, observando que a empresa adota uma abordagem proativa ao implementar serviços de monitoramento que oferecem proteção e gerenciamento as fontes de informação.

Os dados são tratados adequadamente, tanto internamente quanto externamente, por meio de estratégias sólidas de segurança, com o uso de Firewall’s, VPN’s e MFA (*Multi-Factor Authentication*), visando mitigar incidentes e reforçar a proteção, garantindo um ambiente

confiável para a troca e manipulação de informações sensíveis.

### 4.1.1 Adaptabilidade as políticas

De acordo com os registros analisados, a empresa possui uma abordagem que busca o alinhamento com cada responsável pelo produto a ser desenvolvido, visando políticas e tratamento de dados dedicadas ao princípio dos projetos, enaltecendo sua flexibilidade em atender às normas gerais de conformidade e às necessidades de cada cliente utilizando abordagens que variam desde a utilização de VPNs até a liberação de acesso via diretivas específicas de rede.

### 4.1.2 Enfoque na postura

Os compromissos da empresa, segundo os documentos analisados, reforçam a conformidade normativa e a segurança de dados, onde em sua postura demonstra que as decisões tomadas pelo arquiteto de produto são norteadas pelo objetivo de cumprir as exigências regulatórias e proteger as informações de maneira integral como a escolha de ferramentas e de políticas.

Garantindo assim, um serviço confiável e ajustado às particularidades de cada cliente com qualidade e confiança na entrega dos projetos.

## 4.2 Monitoramento seguro

No caso analisado, a empresa demonstrou que um monitoramento proativo e bem estruturado fortalece a postura organizacional em relação à proteção de dados sensíveis no combate a ameaças cibernéticas, especialmente em ambientes que lidam com informações críticas e recursos computacionais intensivos.

A empresa enfrentou um ataque sofisticado envolvendo o *software* malicioso Perfctl que utilizou rootkits para manter-se persistentemente oculto no ambiente, onde a detecção precoce dessa anomalia foi possível graças ao uso das ferramentas de monitoramento e alertas configurados no Zabbix que identificaram um comportamento anômalo de uso elevado e constante de CPU, despertando a atenção da equipe que aprofundou a investigação e encontrou evidências diretas do *malware*, evidenciando a ação preventiva do monitoramento seguro.

Durante a investigação do incidente, o Zabbix desempenhou um papel crucial ao

gerar alertas configurados para detectar uso anômalo de CPU nos servidores afetados. Esses alertas permitiram uma análise detalhada que revelou a presença do *malware* **Perfctl**. A resposta ao incidente incluiu o isolamento imediato das máquinas comprometidas, ajustes na firewall para evitar novas tentativas de invasão, e a implementação de autenticação multifatorial (MFA) para reforçar os acessos. Além disso, a integração do Zabbix com ferramentas forenses possibilitou a coleta de evidências detalhadas, como alterações nos arquivos ".profile" do *root* e a identificação de serviços comprometidos, como o "kmodaudit.service".

### 4.2.1 Estratégias de detecção da anomalia

A eficácia na identificação e mitigação da ameaça foi amplamente apoiada pelo uso de ferramentas e processos bem estruturados, com destaque ao papel do Zabbix no monitoramento contínuo do ambiente, onde no caso analisado demonstrou-se como primordial, pois com suas funcionalidades avançadas de monitoramento, alertas configuráveis e integração com outras ferramentas de segurança, foi possível detectar e responder rapidamente à anomalia identificada.

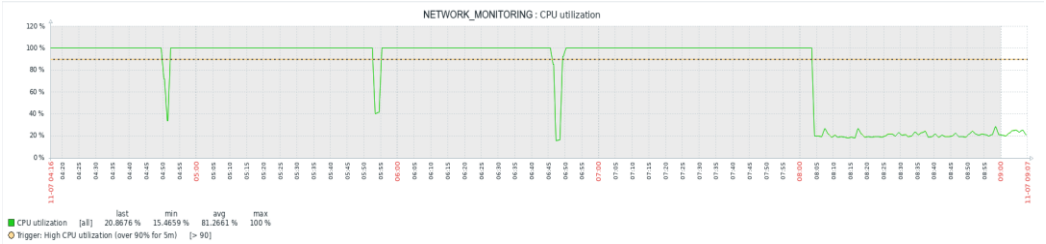
### 4.2.2 O Zabbix como pioneiro na detecção da anomalia

O Zabbix desempenhou um papel crucial como ferramenta de monitoramento contínuo e detecção de anomalias na rede analisada, onde durante o incidente, o malware apresentou uma utilização elevada e constante de CPU, que cessava apenas quando o servidor era acessado via SSH. Além disso, a integração do Zabbix com ferramentas de análise forense e registros de logs potencializou a investigação, permitindo uma correlação precisa entre os eventos detectados e as evidências encontradas nos servidores.

Essa particularidade foi prontamente identificada pela solução, que associou o padrão ao comportamento suspeito, conforme a figura 1 especifica, que por motivos de privacidade foi alterada passando por um processo de anonimização.

.

**Figura 1** - Uso excessivo de recursos da máquina




**Fonte**: Empresa analisada, Documentos.

O sistema foi configurado com alertas altamente customizados, possibilitando notificações imediatas sobre variações nos padrões usuais de desempenho, onde por meio desses alertas o uso prolongado de CPU foi identificado e prontamente habilitado como fruto de atividade maliciosa.

Após os alertas gerados, os analistas correlacionaram dados históricos com o comportamento identificado, permitindo a validação da presença do *malware* e a implementação imediata de contramedidas, onde entre as ações tomadas, destacaram-se o isolamento das máquinas afetadas, ajustes nas configurações de firewall e o fortalecimento dos mecanismos de autenticação, incluindo o uso de múltiplos fatores de verificação.

A eficácia do Zabbix em monitorar continuamente o ambiente foi determinante para mitigar os impactos causados pelo *Perfctl*, onde o *malware* poderia ter operado por mais tempo, comprometendo seriamente a infraestrutura e expondo informações críticas.

Este cenário evidencia a importância de ferramentas avançadas como o Zabbix, que não apenas detectam anomalias de forma ágil, mas também apoiam análises detalhadas e contribuem para a evolução constante da segurança tecnológica, combinando ao monitoramento contínuo as notificações configuráveis e integração com sistemas complementares, consolidando sua posição como uma solução indispensável para ambientes de redes de computadores à riscos cibernéticos.

A análise desse caso demonstrou como o monitoramento contínuo e a configuração adequada de ferramentas como o Zabbix podem reduzir drasticamente o impacto de incidentes cibernéticos. Ao correlacionar dados históricos com eventos em tempo real, a empresa foi capaz de neutralizar a ameaça antes que ela causasse danos significativos à infraestrutura. Esse caso reforça a importância de integrar tecnologias avançadas, políticas de segurança e equipes preparadas em um ecossistema de defesa cibernética eficaz.

### 4.2.3 Tratamento da anomalia

A partir das informações captadas pelo Zabbix, foi possível tratar a ameaça de forma eficiente, removendo o *malware* e reforçando as medidas de segurança no ambiente.

No contexto da ameaça causada pelo malware *Perfctl*, a estratégia utilizada para mitigação e contenção da anomalia foi baseada em um monitoramento contínuo, aliado a processos estruturados de resposta a incidentes, onde a partir dessa identificação, as máquinas comprometidas foram imediatamente isoladas para conter a propagação da ameaça, enquanto ajustes no firewall e reforço da autenticação multifatorial (MFA) foram implementados para aumentar as camadas de proteção.

O padrão observado de uso elevado de CPU por meio de um monitoramento continuo reforçou que reduzia drasticamente a utilização dos recursos ao efetuar o acesso ao servidor, onde foi captado pelos *triggers* configurados na plataforma que por sua vez geraram alertas em tempo real para a equipe de segurança que prontamente atuou para validar os logs, registrados pela figura 2 que por motivos de privacidade foi alterada passando por um processo de anonimização.[AC1]

**Figura 2** - Registro de Logs do Sistema Relacionados ao Malware Perfctl


**Fonte**: Empresa analisada, Documentos.

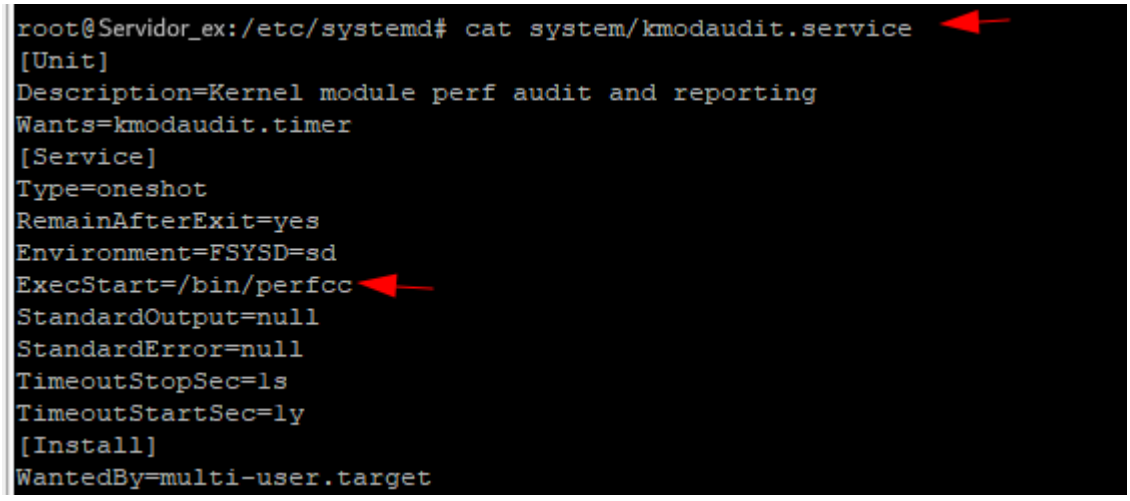
Permitindo assim, apoiar a análise de padrões históricos para identificar a origem e o impacto da anomalia, garantindo uma resposta ágil e direcionada aos dispositivos de persistência presentes no sistema implementados pelo *software* malicioso, com base nos logs foi dectecado um script executável conforme a figura 3 demonstra, por razões de confidencialidade, foi modificada por meio de um processo de desidentificação.

**Figura 3** - Script malicioso autoexecutável


**Fonte**: Empresa analisada, Documentos.

No contexto do tratamento da anomalia, o Zabbix forneceu dados de maneira detalhada, permitindo que auxiliaram na investigação e tratamento do incidente suas funcionalidades de monitorar em tempo real o consumo anômalo de recursos e correlacionar esses dados com os horários de atividade do servidor fosse consumada com o objetivo de registrar eventos críticos nos logs de sistema, que posteriormente foram cruzados com as evidências encontradas no ambiente, como alterações no arquivo .profile do root e serviços comprometidos, como kmodaudit.service. Conforme demonstrado na figura 4, a imagem foi ajustada para preservar a anonimização e mitigar riscos de vazamento de dados.

**Figura 4** - Persistência do malware




**Fonte**: Empresa analisada, Documentos.

Esse caso destaca como o Zabbix, quando bem configurado e integrado a processos

de segurança, torna-se uma ferramenta indispensável para a detecção e mitigação de incidentes em tempo real, assegurando a continuidade das operações e a proteção do ambiente organizacional.

A análise do incidente com o malware *Perfctl* evidenciou aprendizados valiosos sobre a importância do monitoramento contínuo e da integração tecnológica na segurança de redes de computadores.

Primeiramente, ficou claro que monitorar constantemente padrões de uso e comportamento dos sistemas permite identificar anomalias antes que elas causem impactos significativos. Além disso, a integração entre ferramentas avançadas, como o Zabbix, e sistemas de análise forense demonstrou ser essencial para uma investigação detalhada e uma resposta corretiva eficiente. Por fim, destacou-se a relevância de manter políticas de segurança robustas e adaptáveis, como o uso de VPNs, firewalls bem configurados e autenticação multifator, que minimizam as vulnerabilidades exploráveis por agentes maliciosos. Esses aprendizados consolidam o monitoramento de redes como um pilar central na estratégia de segurança da informação, enfatizando a necessidade de investimentos contínuos em tecnologias inovadoras e capacitação das equipes.

### 4.3 Segurança da informação na empresa

A segurança da informação na organização é definida por uma abordagem estratégica que combina a tecnologia de processos estruturados e conscientização contínua dos colaboradores, integrando a proteção da confidencialidade, integridade e disponibilidade dos dados, permitindo mitigar riscos internos e externos em um cenário de ameaças cada vez mais sofisticadas.

A implementação de políticas de controle de acesso específicas para cada cliente, aliada ao uso de tecnologias como autenticação multifatorial (MFA), firewall configuráveis e redes privadas virtuais (VPN), garantiu uma barreira robusta contra acessos não autorizados, onde essas medidas foram complementadas por auditorias regulares que avaliaram e ajustaram continuamente as práticas adotadas, garantindo conformidade com padrões reconhecidos de governança da informação.

Treinamentos regulares sobre boas práticas, detecção de phishing e manipulação segura de dados foram integrados às estratégias de proteção, reduzindo significativamente os riscos associados a erros humanos, onde por meio desse investimento em educação foi possível

criar uma camada adicional de defesa.

A análise pós-incidente destacou a eficácia do modelo integrado da organização utilizando um sistema centralizado de registros de ações no ambiente, permitindo a reconstrução detalhada das etapas do ataque, identificando as vulnerabilidades exploradas e oferecendo insumos para melhorias contínuas na arquitetura de proteção. Além disso, a resposta rápida ao ataque demonstrou que a estrutura da empresa está alinhada às melhores práticas do setor, minimizando o impacto de ameaças e garantindo a continuidade das operações.

Ao adotar uma postura proativa e adaptável, a empresa demonstrou capacidade de lidar com um cenário cibernético em constante evolução. Ferramentas como o Zabbix desempenharam papéis complementares, enquanto os processos internos e a interação humana reforçaram os pontos críticos de segurança.

O equilíbrio entre tecnologia e estratégia organizacional se traduziu em um modelo de gestão da segurança da informação robusto e escalável, evidenciando a importância de uma abordagem integrada para proteção de ativos digitais, combinando tecnologia, políticas e engajamento humano, onde essa estratégia não apenas respondeu de forma eficaz ao ataque, mas também preparou a empresa para enfrentar ameaças futuras, posicionando-a como referência em gestão de segurança da informação.

### 4.4 Uso de centros de operações de segurança (*SOC*) e rede de computadores (*NOC*)

O uso integrado de Centros de Operações de Segurança (*SOC - Security Operations Center*) e Centros de Operações de Rede (*NOC - Network Operations Center*) desempenha um papel crucial na gestão da segurança e na estabilidade de redes de computadores, pois o *SOC* se concentra em monitorar e responder a ameaças cibernéticas e o *NOC* é responsável por garantir o desempenho e a disponibilidade da infraestrutura de rede, funcionando como peças complementares de uma estratégia abrangente de segurança da informação.

No estudo de caso, o *SOC* da empresa desempenhou um papel essencial na identificação e mitigação do incidente envolvendo o *malware* Perfctl, onde a equipe do *SOC* monitorava continuamente o ambiente em busca de anomalias, utilizando ferramentas como o Zabbix para alertar sobre padrões de comportamento incomuns e, assim que o alerta sobre o uso elevado de CPU foi gerado, o *SOC* iniciou a análise detalhada do incidente, colaborando com o NOC para isolar os sistemas afetados e restaurar a funcionalidade da rede.

Por outro lado, o *NOC* garantiu a estabilidade operacional durante o tratamento do

incidente, ajustando configurações de rede e priorizando o tráfego legítimo enquanto as máquinas comprometidas eram isoladas, onde a coordenação entre *SOC* e *NOC* foi essencial para minimizar os impactos na operação da empresa e assegurar a continuidade dos serviços.

Essa integração promove uma abordagem preventiva e reativa às ameaças no caso analisado para o sucesso das medidas de contenção e recuperação, onde o estudo evidenciou que a centralização do monitoramento e da segurança em um *SOC* bem estruturado proporciona maior capacidade de resposta a incidentes e maior eficiência na análise de logs e padrões de comportamento, por sua vez combinado ao suporte técnico do *NOC*, a empresa conseguiu lidar com o ataque de forma eficaz, demonstrando a importância de equipes especializadas e ferramentas tecnológicas de ponta para enfrentar os desafios de um ambiente digital em constante evolução, quando associada a tecnologias avançadas e processos bem definidos, forma a base de uma estratégia robusta de segurança da informação, capaz de proteger redes de computadores contra ameaças crescentes e garantir a continuidade das operações críticas.

## 5. CONCLUSÃO

A segurança da informação, quando aplicada ao monitoramento de redes de computadores, se estabelece como um elemento indispensável para a proteção de dados e a continuidade operacional em um cenário digital em constante evolução. Este estudo demonstrou como práticas estruturadas e o monitoramento contínuo, sustentados pelos pilares de confidencialidade, integridade e disponibilidade, podem prevenir incidentes graves e mitigar ameaças cibernéticas, evidenciando a importância de estratégias proativas e adaptáveis.

O estudo de caso analisado revelou a eficácia de processos bem definidos na detecção e contenção de anomalias, reforçando que o monitoramento contínuo permite identificar ameaças antes que causem impactos significativos. Além disso, foi destacada a relevância da conformidade com normas internacionais, como a *ISO/IEC 27001* e *27002*, que fornecem diretrizes fundamentais para uma gestão segura e eficiente.

A partir dos aprendizados extraídos, ficou evidente que integrar políticas de segurança robustas, ferramentas tecnológicas avançadas e equipes capacitadas é essencial para enfrentar os desafios impostos por um ambiente cibernético cada vez mais complexo. Este trabalho não apenas consolidou o papel do monitoramento de redes como um pilar da segurança da informação, mas também reforçou a necessidade de investimentos constantes em inovação, capacitação e melhoria contínua dos processos. Assim, reforça-se a relevância de uma

abordagem integrada e estratégica para a construção de infraestruturas digitais resilientes e confiáveis.

## REFERÊNCIAS


ANDREW, S. T.; DAVID, J. W. **Computer networks**. 5. ed. Prentice Hall, 2011.

BASSO, D. E. **Administração de redes de computadores**. São Paulo: Contentus, 2020.

COMER, D. E. **Redes de computadores e internet**. 6. ed. Porto Alegre: Bookman, 2016.
HINTZBERGEN, Jule; HINTZBERGEN, Kees; SMULDERS, André; BAARS, Hans. **Fundamentos de segurança da informação: com base na ISO 27001 e na ISO 27002**. Rio de Janeiro: Brasport, 2018.

ISO/IEC. **Information security, cybersecurity and privacy protection — Information security controls**. 3. ed. Geneva: International Organization for Standardization, 2022.

ISO/IEC. **Information security, cybersecurity and privacy protection — Information security management systems — Requirements**. 3. ed. Geneva: International Organization for Standardization, 2022.

KOSTOPOULOS, G. **Cyberspace and cybersecurity**. Auerbach Publications, 2017.

KUROSE, J.; ROSS, K. **Computer networking: a top-down approach**. 6. ed. Boston: Pearson, 2013.

NIELES, Michael; DEMPSEY, Kelley; PILLITTERI, Victoria Yan. **An introduction to information security**. NIST Special Publication 800.12, 2017.

SAYDAM, T.; MAGEDANZ, T. **From networks and network management into service and service management**. *Journal of Networks and System Management*, 1996.

SOUSA, Manoel Veras de. **Redes de computadores: fundamentos e práticas**. Rio de Janeiro: Brasport, 2013.

STALLINGS, William; BROWN, Lawrie. **Computer security: principles and practice**. Pearson, 2015.

TANENBAUM, Andrew S. **Redes de computadores**. 3. ed. Rio de Janeiro: Campus, 1996.

ZABBIX. **Documentation 6.0**. 20 nov. 2024. Disponível em: https://www.zabbix.com/documentation/6.0/pt. Acesso em: 21 nov. 2024.

ZIMMERMAN, C. **Cybersecurity operations center**. The MITRE Corporation, 2014.