INSTITUTO FEDERAL
Rondônia

MINISTÉRIO DA EDUCAÇÃO
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia de Rondônia

IFRO Campus Porto Velho Zona Norte
Coordenação do Curso Redes de computadores

CIBELY SOUZA CHUINCA

ROMOLO GARCIA TIBÚRCIO

Segurança em Ambientes Virtualizados: O Uso do Linux na Proteção de Infraestruturas de Rede

PORTO VELHO
2026

CIBELY SOUZA CHUINCA

ROMOLO GARCIA TIBÚRCIO

Segurança em Ambientes Virtualizados: O Uso do Linux na Proteção de Infraestruturas de Rede

Artigo entregue como Trabalho de Conclusão de Curso ao Instituto Federal de Educação, Ciência e Tecnologia de Rondônia (IFRO), *Campus* Porto Velho Zona Norte, como requisito parcial para obtenção do grau de tecnólogo, junto ao Curso Redes de Computadores, sob a orientação do professor Me. Silmar Antônio Buchner de Oliveira.

PORTO VELHO
2026

Ficha catalográfica elaborada pelo Sistema Gerador de Ficha Catalográfica do IFRO.

Chuinca, Cibely Souza.
Segurança em ambientes virtualizados: o uso do Linux na proteção de infraestruturas de rede / Cibely Souza Chuinca, Rômolo Garcia Tibúrcio. - Porto Velho, 2026.
15 f.

Orientador(a): Prof. Me. Silmar Antonio Buchner de Oliveira.

Trabalho de Conclusão de Curso (Superior de Tecnologia em Redes de Computadores) – Instituto Federal de Educação, Ciência e Tecnologia de Rondônia - IFRO, Porto Velho, 2026.

1. Virtualização. 2. Linux. 3. Data center. 4. Proteção de dados. 5. Administração de redes. I. Tibúrcio, Rômolo Garcia. II. Oliveira, Silmar Antonio Buchner de (orient.). III. Instituto Federal de Educação, Ciência e Tecnologia de Rondônia - IFRO. IV. Título.

Bibliotecário(a) Responsável: Celia Reis Sales, CRB-CRB11/955

CIBELY SOUZA CHUINCA

ROMOLO GARCIA TIBÚRCIO

Segurança em Ambientes Virtualizados: O Uso do Linux na Proteção de Infraestruturas de Rede

Artigo entregue como Trabalho de Conclusão de Curso ao Instituto Federal de Educação, Ciência e Tecnologia de Rondônia (IFRO), Campus Porto Velho Zona Norte, como requisito para obtenção do título de Tecnólogo em Redes de Computadores.

Aprovado em: 30/06/2026 pela banca examinadora.

gov.br
Documento assinado digitalmente
SILMAR ANTONIO BUCHNER DE OLIVEIRA
Data: 28/07/2026 14:37:06-0300
Verifique em https://validar.iti.gov.br

Silmar Antonio Buchner de Oliveira

Orientador

gov.br
Documento assinado digitalmente
RENATO ALMEIDA DE OLIVEIRA
Data: 28/07/2026 14:40:32-0300
Verifique em https://validar.iti.gov.br

Renato Almeida de Oliveira

Examinador Interno

gov.br
Documento assinado digitalmente
JHORDANO MALACARNE BRAVIM
Data: 28/07/2026 15:09:17-0300
Verifique em https://validar.iti.gov.br

Jhordano Malacarne Bravim

Examinador Interno

Segurança em Ambientes Virtualizados: O Uso do Linux na Proteção de Infraestruturas de Rede

RESUMO: A virtualização permite a execução de múltiplos sistemas operacionais em uma mesma infraestrutura física, tornando-se uma tecnologia essencial em ambientes computacionais modernos. Este trabalho analisa a contribuição do Linux para a segurança de infraestruturas de rede virtualizadas, destacando seus mecanismos de proteção e sua aplicação na mitigação de ameaças cibernéticas. A pesquisa foi desenvolvida por meio de revisão bibliográfica de livros especializados sobre virtualização, segurança da informação e sistemas Linux. Os resultados indicam que recursos como controle de permissões, firewalls e ferramentas de monitoramento fortalecem a proteção dos ambientes virtualizados e contribuem para a mitigação de ameaças cibernéticas. Conclui-se que o Linux desempenha papel fundamental na segurança de infraestruturas virtualizadas, especialmente quando aliado a boas práticas de configuração e gerenciamento.

PALAVRAS-CHAVE: Virtualização; Linux; Data Center; proteção de dados; administração de redes.

ABSTRACT: Virtualization enables the execution of multiple operating systems on the same physical infrastructure, making it an essential technology in modern computing environments. This study analyzes Linux's contribution to the security of virtualized network infrastructures, highlighting its protection mechanisms and its application in mitigating cyber threats. The research was conducted through a literature review of specialized books on virtualization, information security, and Linux systems. The results indicate that features such as permission controls, firewalls, and monitoring tools strengthen the protection of virtualized environments and contribute to cyber threat mitigation. It is concluded that Linux plays a fundamental role in the security of virtualized infrastructures, especially when combined with best practices for configuration and management.

KEYWORDS: Virtualization; Linux; Data Center; data protection; network administration.

1 INTRODUÇÃO

A crescente utilização de tecnologias da informação nas organizações tem impulsionado a adoção de ambientes virtualizados como forma de otimizar recursos computacionais, reduzir custos e aumentar a eficiência na gestão de infraestruturas de rede. Nesse contexto, a virtualização permite a execução de múltiplos sistemas operacionais em uma mesma máquina física, promovendo maior flexibilidade e melhor aproveitamento dos recursos disponíveis, conforme destacado por Tanenbaum e Bos (2016).

Apesar dos benefícios proporcionados por essa tecnologia, também surgem desafios significativos relacionados à segurança da informação, uma vez que ambientes virtualizados podem ampliar a superfície de ataque e aumentar os riscos de vulnerabilidades, acessos não autorizados e falhas de configuração. Segundo Nakamura e Geus (2007), a proteção de redes e sistemas deve garantir a confidencialidade, integridade e disponibilidade das informações, especialmente em ambientes complexos e interconectados.

Diante disso, o sistema operacional Linux destaca-se como uma importante ferramenta na proteção de infraestruturas de rede, devido aos seus mecanismos de segurança, estabilidade e ampla utilização em servidores e ambientes corporativos. De acordo com Negus (2020), o Linux oferece recursos como controle de permissões, autenticação de usuários, firewalls e sistemas avançados de segurança, como SELinux, que contribui para o fortalecimento da proteção dos sistemas.

Assim, o presente trabalho trata da análise da contribuição do sistema operacional Linux na proteção de infraestruturas de rede em ambientes virtualizados, buscando compreender como seus mecanismos de segurança podem auxiliar na mitigação de riscos e vulnerabilidades nesses ambientes.

A relevância deste estudo está relacionada ao aumento da dependência das organizações em relação às infraestruturas digitais e à necessidade de proteção contra ameaças cibernéticas cada vez mais sofisticadas. Dessa forma, compreender

o papel do Linux na segurança de ambientes virtualizados torna-se fundamental para

o desenvolvimento de práticas mais seguras e eficientes na gestão de redes.

Diante desse cenário, este trabalho tem como objetivo geral analisar a contribuição do sistema operacional Linux na proteção de infraestruturas de rede em ambientes virtualizados. Como objetivos específicos, busca-se compreender os conceitos de virtualização e ambientes virtualizados, identificar os principais riscos e vulnerabilidades em infraestruturas de rede, analisar os mecanismos de segurança oferecidos pelo Linux e avaliar sua contribuição na mitigação de ameaças e fortalecimento da segurança da informação.

2 REFERENCIAL TEÓRICO

2.1 VIRTUALIZAÇÃO E INFRAESTRUTURA DE REDE

A virtualização é uma tecnologia amplamente utilizada nas organizações modernas por permitir a execução de múltiplos sistemas operacionais em um único equipamento físico. Segundo Stallings (2018), a virtualização possibilita melhor aproveitamento dos recursos computacionais, reduzindo custos operacionais e aumentando a flexibilidade da infraestrutura de Tecnologia da Informação (TI).

De acordo com Morimoto (2010), a virtualização consiste na criação de ambientes computacionais independentes, chamados máquinas virtuais, que compartilham os recursos de hardware de um servidor físico. Essa tecnologia tem sido adotada por empresas de diferentes portes devido à facilidade de gerenciamento e à otimização dos recursos disponíveis.

Para Nunes (2019), a virtualização também contribui para a escalabilidade das infraestruturas de rede, permitindo a rápida criação e configuração de novos serviços sem a necessidade de aquisição imediata de novos equipamentos.

Além dos benefícios relacionados ao desempenho e à economia, a virtualização tornou-se um elemento fundamental em ambientes corporativos, especialmente em data centers e serviços de computação em nuvem (TANENBAUM; BOS, 2016).

2.2 SEGURANÇA EM AMBIENTES VIRTUALIZADOS

Embora a virtualização ofereça inúmeras vantagens, ela também introduz

novos desafios relacionados à segurança da informação. Conforme explica Stallings (2018), a concentração de diversos serviços em um único host físico pode aumentar os impactos causados por falhas de segurança, caso não existam mecanismos adequados de proteção.

Segundo Sêmola (2014), a segurança da informação está fundamentada nos princípios da confidencialidade, integridade e disponibilidade dos dados. Em ambientes virtualizados, esses princípios devem ser aplicados tanto às máquinas virtuais quanto aos servidores físicos que as hospedam.

De acordo com Nakamura e Geus (2007), ameaças como acessos não autorizados, falhas de configuração, exploração de vulnerabilidades e ataques direcionados ao hipervisor podem comprometer toda a infraestrutura virtualizada.

Para Fontes (2017), a adoção de políticas de segurança, controles de acesso, monitoramento contínuo e atualizações frequentes são práticas essenciais para reduzir riscos em ambientes virtualizados.

2.3 O SISTEMA OPERACIONAL LINUX

O Linux é um sistema operacional de código aberto amplamente utilizado em servidores e ambientes corporativos devido à sua estabilidade, desempenho e segurança. Segundo Nemeth et al. (2017), o Linux destaca-se pela robustez de sua arquitetura e pela grande capacidade de personalização oferecida aos administradores de sistemas.

Conforme explica Shotts (2019), uma das principais características do Linux é o controle rigoroso de permissões de arquivos e diretórios, permitindo limitar o acesso dos usuários aos recursos do sistema.

De acordo com Morimoto (2010), a natureza open source do Linux possibilita auditorias constantes no código-fonte, contribuindo para a identificação e correção rápida de vulnerabilidades.

Além disso, o Linux possui ampla compatibilidade com ferramentas de segurança, servidores, firewalls e soluções de virtualização, tornando-se uma das principais escolhas para ambientes corporativos (NEGUS, 2020).

2.4 O USO DO LINUX NA PROTEÇÃO DE INFRAESTRUTURAS DE REDE

O Linux desempenha um papel importante na proteção de infraestruturas de rede por disponibilizar mecanismos avançados de segurança nativamente integrados ao sistema operacional. Segundo Nemeth et al. (2017), ferramentas como controle de permissões, autenticação de usuários e gerenciamento de serviços permitem aumentar significativamente a proteção dos ambientes computacionais.

Conforme destaca Shotts (2019), o firewall Netfilter, administrado por meio do IPTables ou do NFTables, possibilita controlar o tráfego de rede, bloquear acessos indevidos e aplicar políticas de segurança personalizadas.

De acordo com Fontes (2017), a utilização de logs de sistema e ferramentas de monitoramento auxilia na identificação precoce de incidentes de segurança e comportamentos anormais na rede.

Outra importante funcionalidade é a utilização do SELinux (Security-Enhanced Linux), desenvolvido pela Agência Nacional de Segurança dos Estados Unidos (NSA), que adiciona camadas extras de controle de acesso aos recursos do sistema operacional (STALLINGS, 2018).

2.5 BOAS PRÁTICAS DE SEGURANÇA EM AMBIENTES VIRTUALIZADOS COM LINUX

A adoção de boas práticas é fundamental para garantir a segurança dos ambientes virtualizados. Segundo Nakamura e Geus (2007), a atualização constante dos sistemas operacionais e softwares reduz a exposição a vulnerabilidades conhecidas.

De acordo com Fontes (2017), recomenda-se a implementação de mecanismos de autenticação forte, segmentação de redes, utilização de firewalls e realização periódica de backups.

Para Stallings (2018), o monitoramento contínuo dos ambientes virtualizados permite detectar falhas de segurança antes que elas causem impactos significativos à organização.

Além disso, Sêmola (2014), destaca que a conscientização dos usuários e administradores é um fator essencial para a manutençao da segurança da informação, uma vez que muitos incidentes decorrem de falhas humanas.

2.6 PRINCIPAIS AMEAÇAS À SEGURANÇA EM AMBIENTES VIRTUALIZADOS

Os ambientes virtualizados oferecem diversos benefícios para as organizações, porém também apresentam desafios específicos relacionados à segurança da informação. Segundo Stallings (2018), a consolidação de múltiplos serviços em um único servidor físico pode aumentar os impactos causados por falhas de segurança, tornando necessária a adoção de mecanismos de proteção adequados.

Entre as principais ameaças presentes nesses ambientes destacam-se os ataques direcionados às máquinas virtuais, vulnerabilidades no hipervisor e falhas de configuração.

De acordo com Nakamura e Geus (2007), configurações inadequadas podem permitir acessos não autorizados e comprometer a integridade dos sistemas hospedados em ambientes virtualizados.

Outra ameaça relevante é a propagação de malwares e ransomwares. Conforme Sêmola (2014), esses softwares maliciosos podem comprometer dados importantes da organização, causando indisponibilidade dos serviços e prejuízos financeiros significativos. Em ambientes virtualizados, uma infecção pode afetar várias máquinas virtuais simultaneamente, ampliando os danos causados pelo ataque.

Segundo Fontes (2017), a utilização inadequada de credenciais administrativas representa um dos principais fatores de risco para a segurança da informação. O uso de senhas fracas, compartilhamento de acessos e ausência de políticas de autenticação favorecem a ocorrência de incidentes de segurança.

De acordo com Tanenbaum e Bos (2016), os hipervisores também podem se tornar alvos de ataques cibernéticos, uma vez que são responsáveis pelo gerenciamento das máquinas virtuais. Caso um invasor obtenha acesso ao hipervisor, poderá comprometer diversas máquinas virtuais hospedadas no mesmo ambiente.

Além disso, a falta de atualizações de segurança representa um risco significativo. Conforme Nemeth et al. (2017), sistemas desatualizados tendem a apresentar vulnerabilidades conhecidas que podem ser exploradas por atacantes para obtenção de acesso indevido aos recursos computacionais.

Para Stallings (2018), a identificação e mitigação dessas ameaças dependem

da implementação de controles de segurança adequados, monitoramento contínuo e aplicação de políticas que garantam a proteção dos ativos de informação.

2.7 FERRAMENTAS DE SEGURANÇA DO LINUX PARA PROTEÇÃO DE REDES

O sistema operacional Linux disponibiliza diversas ferramentas voltadas para a proteção de redes e sistemas computacionais. Segundo Nemeth et al. (2017), a combinação de recursos nativos e softwares especializados torna o Linux uma das principais plataformas utilizadas em ambientes corporativos que exigem elevados níveis de segurança.

Entre as ferramentas mais utilizadas destaca-se o IPTables, responsável pelo gerenciamento das regras de firewall do sistema. De acordo com Shotts (2019), essa ferramenta permite controlar o tráfego de entrada e saída da rede, bloqueando conexões não autorizadas e reduzindo a exposição a ameaças externas.

Conforme Morimoto (2010), o IPTables possibilita a criação de políticas de filtragem personalizadas, permitindo que os administradores definam regras específicas para cada serviço disponibilizado na rede.

Outra solução amplamente utilizada é o NFTables, considerado uma evolução do IPTables. Segundo Negus (2020), essa ferramenta oferece maior flexibilidade e desempenho no gerenciamento de regras de firewall, tornando-se uma alternativa moderna para proteção de ambientes Linux.

O SELinux (Security-Enhanced Linux) representa outro importante mecanismo de segurança. Desenvolvido originalmente pela NSA, ele adiciona uma camada extra de controle de acesso ao sistema operacional. De acordo com Stallings (2018), o SELinux restringe as ações que podem ser executadas pelos processos, minimizando os impactos causados por invasões e falhas de segurança.

Segundo Fontes (2017), o monitoramento contínuo constitui um dos pilares da segurança da informação. Nesse contexto, os registros de eventos (logs) gerados pelo Linux permitem identificar tentativas de acesso indevido, falhas operacionais e atividades suspeitas.

Além disso, o Linux oferece suporte a ferramentas como o Fail2Ban, utilizado

para proteção contra ataques de força bruta. Conforme Shotts (2019), essa ferramenta monitora tentativas repetidas de autenticação e bloqueia automaticamente endereços IP considerados suspeitos.

De acordo com Morimoto (2010), o OpenSSH também desempenha papel fundamental na segurança dos ambientes Linux, permitindo conexões remotas criptografadas e protegidas contra interceptação de dados.

Outro recurso relevante é o sistema de permissões de arquivos e diretórios. Segundo Nemeth et al. (2017), o modelo de controle de acesso do Linux permite limitar as ações dos usuários, reduzindo o risco de alterações indevidas ou vazamento de informações.

Para Sêmola (2014), a utilização conjunta dessas ferramentas fortalece significativamente a segurança das infraestruturas de rede, contribuindo para a proteção da confidencialidade, integridade e disponibilidade das informações.

3 METODOLOGIA

A presente pesquisa caracteriza-se como uma pesquisa bibliográfica, de natureza aplicada e abordagem qualitativa, desenvolvida com o objetivo de analisar a importância do sistema operacional Linux na proteção de infraestruturas de rede em ambientes virtualizados.

Segundo Gil (2019), a pesquisa bibliográfica é elaborada com base em materiais já publicados, como livros especializados, permitindo ao pesquisador aprofundar seus conhecimentos sobre determinado tema.

Em relação aos objetivos, trata-se de uma pesquisa descritiva, pois procura descrever as características da virtualização, dos mecanismos de segurança presentes no sistema operacional Linux e sua aplicação na proteção de infraestruturas de rede. De acordo com Gil (2019), a pesquisa descritiva tem como finalidade observar, registrar e analisar fenômenos sem interferir diretamente em sua ocorrência.

A coleta de dados foi realizada por meio de levantamento bibliográfico em livros especializados sobre virtualização, segurança da informação e sistemas operacionais Linux.

Em bases de dados como o Google Acadêmico, além de publicações relacionadas às áreas de segurança da informação, virtualização e sistemas operacionais Linux. Inicialmente, foram identificadas diversas obras relacionadas ao tema da pesquisa. Em seguida, realizou-se um processo de seleção, considerando como critérios a relevância para os objetivos do estudo, a abordagem sobre virtualização, segurança da informação e Linux, bem como a credibilidade dos autores e das publicações. Foram priorizados livros de referência que apresentavam conteúdo diretamente relacionado ao tema, sendo descartadas as obras que não tratavam especificamente da segurança em ambientes virtualizados ou que não contribuíam para responder aos objetivos da pesquisa.

4 RESULTADOS E DISCUSSÕES

Este capítulo apresenta os resultados obtidos por meio da revisão bibliográfica realizada sobre a segurança em ambientes virtualizados e o uso do sistema operacional Linux na proteção de infraestruturas de rede. A análise das obras consultadas permitiu responder ao objetivo geral da pesquisa e demonstrar como cada objetivo específico foi alcançado.

O primeiro objetivo específico consistiu em compreender os conceitos de virtualização e ambientes virtualizados. A literatura analisada demonstrou que a virtualização permite a execução de diversos sistemas operacionais em um único equipamento físico, promovendo melhor aproveitamento dos recursos computacionais, redução de custos e maior flexibilidade na administração da infraestrutura de Tecnologia da Informação. Os estudos de Stallings (2018), Morimoto (2010) e Tanenbaum e Bos (2016) mostram que essa tecnologia se tornou essencial para organizações que buscam eficiência, escalabilidade e disponibilidade de serviços.

O segundo objetivo foi identificar os principais riscos e vulnerabilidades em infraestruturas de rede. A pesquisa evidenciou que ambientes virtualizados estão sujeitos a ameaças como ataques direcionados às máquinas virtuais, vulnerabilidades no hipervisor, falhas de configuração, acessos não autorizados, malwares e ransomwares. Também foi observado que a ausência de atualizações de segurança

e o uso inadequado de credenciais administrativas aumentam significativamente os riscos de incidentes, conforme discutido por Nakamura e Geus (2007), Sêmola (2014) e Fontes (2017).

O terceiro objetivo consistiu em analisar os mecanismos de segurança oferecidos pelo Linux. Os autores pesquisados demonstram que o sistema operacional Linux disponibiliza diversos recursos voltados à proteção das infraestruturas de rede, entre eles o controle de permissões de usuários e arquivos, os firewalls IPTables e NFTables, o SELinux, o OpenSSH, o Fail2Ban e ferramentas de monitoramento por meio de logs. Esses mecanismos contribuem para restringir acessos indevidos, monitorar atividades suspeitas e fortalecer a segurança dos ambientes virtualizados (NEMETH et al., 2017; SHOTTS, 2019; NEGUS, 2020).

O quarto objetivo específico foi avaliar a contribuição do Linux na mitigação de ameaças e no fortalecimento da segurança da informação. Os resultados obtidos indicam que o Linux desempenha papel fundamental na proteção das infraestruturas virtualizadas, principalmente quando utilizado em conjunto com boas práticas de administração, atualização constante dos sistemas, autenticação forte, segmentação de redes e realização de backups periódicos. A literatura consultada demonstra que essas medidas reduzem vulnerabilidades, aumentam a disponibilidade dos serviços e fortalecem os princípios da confidencialidade, integridade e disponibilidade das informações (FONTES, 2017; STALLINGS, 2018).

De modo geral, os resultados obtidos por meio da pesquisa bibliográfica demonstram que o objetivo geral deste trabalho foi alcançado. Ficou evidenciado que a combinação entre virtualização e Linux oferece um ambiente mais seguro, estável e eficiente para a proteção das infraestruturas de rede. Além disso, verificou-se que a adoção das ferramentas de segurança disponibilizadas pelo Linux, aliada à aplicação de boas práticas de gestão da segurança da informação, representa uma estratégia eficaz para minimizar riscos e fortalecer a proteção dos ativos computacionais das organizações.

5 CONSIDERAÇÕES FINAIS

A crescente utilização da virtualização nas organizações tem proporcionado

diversos benefícios, como melhor aproveitamento dos recursos computacionais, redução de custos e maior flexibilidade na gestão das infraestruturas de Tecnologia da Informação. No entanto, a adoção dessa tecnologia também traz desafios relacionados à segurança, tornando necessária a implementação de mecanismos capazes de proteger sistemas, redes e informações contra ameaças e vulnerabilidades.

Neste contexto, o presente trabalho teve como objetivo analisar a importância do sistema operacional Linux na proteção de infraestruturas de rede em ambientes virtualizados. Por meio da pesquisa bibliográfica realizada, foi possível compreender os principais conceitos relacionados à virtualização, identificar os riscos de segurança presentes nesses ambientes e analisar os recursos disponibilizados pelo Linux para a proteção dos sistemas.

Como limitação desta pesquisa, destaca-se o fato de o estudo ter sido desenvolvido exclusivamente por meio de revisão bibliográfica, sem a realização de experimentos práticos em ambientes virtualizados. Assim, os resultados fundamentam-se nas contribuições da literatura especializada.

Como sugestão para trabalhos futuros, recomenda-se a realização de estudos experimentais que avaliem a aplicação dos mecanismos de segurança do Linux em ambientes virtualizados reais, incluindo análises comparativas entre diferentes distribuições Linux, hipervisores e plataformas como o Proxmox VE, ampliando o conhecimento sobre a segurança dessas infraestruturas.

6 REFERÊNCIAS

FONTES, Edison Luiz Gonçalves. Segurança da Informação: o usuário faz a diferença. São Paulo: Saraiva, 2017.

GIL, Antônio Carlos. Métodos e Técnicas de Pesquisa Social. 7. ed. São Paulo: Atlas, 2019.

MORIMOTO, Carlos E. Linux: guia prático. Porto Alegre: Sul Editores, 2010.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício de. Segurança de Redes em Ambientes Cooperativos. São Paulo: Novatec, 2007.

NEGUS, Christopher. Linux Bible. 10. ed. Indianapolis: Wiley, 2020.

NEMETH, Evi et al. UNIX and Linux System Administration Handbook. 5. ed. Boston: Pearson, 2017.

NUNES, Mauro César Bernardes. Virtualização de Servidores e Serviços. São Paulo: Érica, 2019.

SÊMOLA, Marcos. Gestão da Segurança da Informação. 3. ed. Rio de Janeiro: Elsevier, 2014.

SHOTTS, William. The Linux Command Line. 2. ed. San Francisco: No Starch Press, 2019.

STALLINGS, William. Segurança de Computadores: Princípios e Práticas. 6. ed. São Paulo: Pearson, 2018.

TANENBAUM, Andrew S.; BOS, Herbert. Sistemas Operacionais Modernos. 4. ed. São Paulo: Pearson, 2016.