# UTILIZANDO A SOLUÇÃO MIKROTIK NA SEGURANÇA E GERENCIAMENTO DE REDES DE COMPUTADORES

**Mayson Petherson Reis Azevedo**
mayson-reiz@hotmail.com

**José Aprígio Carneiro Neto**
jose.neto@ifs.edu.br

**Wanderson Roger Azevedo Dias**
wradias@gmail.com

**Resumo –** Em redes de computadores, um dos grandes desafios enfrentados é com a questão da segurança. A segurança em redes está associada a mecanismos de hardware e software que visam, na sua implementação, reduzir esses problemas de forma eficaz. Com a presença da Internet no cotidiano das empresas, aumentam as possibilidades de fraudes eletrônicas e ataques externos que exploram vulnerabilidades dos sistemas computacionais utilizados. A medida que se disponibiliza dados e equipamentos ao alcance de várias pessoas, cria-se um ponto de atenção, a segurança para com esses dados. Com o aumento da utilização de componentes de redes e da internet, ocorreu um grande crescimento no número de ataques e infecções por vírus nas redes de computadores, justificando dessa forma à necessidade de investimentos na área de segurança de redes e gerência das redes. Através de um sistema de gerência e segurança de rede integrado, é possível fazer um controle do acesso às informações e recursos concentrado, além de contar com a presença de equipamentos como os firewalls e os proxys, para proteger os sistemas computacionais, através do uso de uma autenticação forte e de encriptação nas informações. Dessa forma, o objetivo desse projeto é construir um ambiente de rede de computadores de alta performance, seguro e de fácil gerenciamento, visando minimizar os problemas de gerenciamento e de falta de segurança na rede.

**Palavras-Chave:** Proteção, Sistemas Computacionais, Configuração, Equipamento.

## INTRODUÇÃO

As redes de computadores surgiram da necessidade de compartilhamento de informações e de outros recursos computacionais, tais como, *hardware* e *software* (TORRES, 2009). À medida que essas redes se desenvolveram, tornou-se comum e indispensável a sua presença em diversas áreas e atividades do nosso cotidiano.

Com o advento da Internet, o volume de informações e de transações envolvendo dados pessoais e de negócios cresceu de forma exponencial, necessitando de uma maior proteção (segurança) e gerenciamento no controle de tráfego dessas informações, a fim de evitar problemas em relação à sua perda ou ao acesso não autorizado às mesmas (TANEMBAUM, 2003).

Como forma de garantir a efetividade na segurança das redes de computadores, é imprescindível a implantação de recursos de segurança baseados no controle dos riscos presentes, identificando às principais ameaças e modificando a segurança da rede de acordo com o tipo e o nível de ameaças (NAKAMURA; GEUS, 2002).

A segurança nas redes de computadores consiste em um método utilizado para proteger o tráfego de informações digitais, bem como seus recursos, proporcionando confiança no sistema computacional (*hardware* e *software*).

De acordo com Kurose e Ross (2009), a segurança de redes de computadores está baseada em quatro objetivos, são eles: confidencialidade, autenticação, integridade e disponibilidade.

Outro ponto que merece destaque no processo de segurança das redes de computadores é com

a política de segurança a ser adotada na rede. "*A política de segurança define os direitos e as responsabilidades de cada um em relação à segurança dos recursos computacionais que utiliza e as penalidades às quais está sujeito, caso não a cumpra*" (CERT. BR, 2019).

A importância da política de segurança é imensurável, tanto para os indivíduos que fazem parte de uma organização, como para a própria organização, tendo em vista que com a política de segurança é possível especificar de forma clara o objetivo esperado para a proteção da rede.

Para Nakamura (2002), a política de segurança pode conter outras políticas específicas, tais como: política de senhas, política de backup, política de privacidade, política de confidencialidade e *Acceptable Use Policy* (*AUP*) - "Termos de Uso".

Diante desse cenário, é fundamental a implantação de mecanismos de proteção (segurança) e de gerenciamento que possam garantir a integridade e a segurança de todas essas informações, bem como a correta utilização dos recursos de *hardware* e *software* dos sistemas computacionais presentes em um rede de computadores. Partindo desse princípio, o objetivo desse trabalho é utilizar uma solução *Mikrotik* para atender a todas essas necessidades, implementando recursos de *NAT*, *Firewall*, *Proxy*, *DNS*, *DHCP*, além de gerenciamento de banda de internet e de usuários.

O *MikroTik* é um *routerOs*, ou seja, um sistema operacional baseado em *Linux*, desenvolvido para realizar a tarefa de um roteador, sendo considerado como um "roteador" de alto desempenho. O *MikroTik* foi desenvolvido em 1997, pela empresa fabricante de equipamentos para redes de computadores *MikroTik*, fundada na Letônia (Rússia), em 1995. A empresa atualmente desenvolve equipamentos *Wireless* e Roteadores, seus equipamentos são muito utilizados por provedores de banda larga e empresas dos mais variados segmentos de TI no mundo todo, além disso, os seus equipamentos são conhecidos pela sua estabilidade e versatilidade.

Atualmente, o *MikroTik* é equipamento de rede muito utilizado em soluções para *ISP* (*Internet Service Provider*), na administração de redes de computadores e de serviços *wireless*, devido a sua grande variedade de características, tais como: desempenho otimizado com o protocolo proprietário *NSTREME*, alta disponibilidade com o protocolo *VRRP*, possibilidade de agregar interfaces (*bonding*), poucas exigências de recursos de *hardware*, qualidade de serviço avançado, *firewall* "*stateful*", protocolo *Spanning Tree* em *bridge* com filtros, alta velocidade com protocolos 802.11 a/b/g com criptografia *WEP/WPA,WDS* e *Aps* virtuais, portal captativo (*Hotspot*) com acesso "*Plug & Play*", roteamento com os protocolos *RIP*, *OSPF* e *BGP*, acesso remoto com amigável aplicativo *windows*, *Winbox* e administração *Web*, administração por *Telnet*, *Mac-Telnet*, *SSH* e console, além de configuração e monitoramento em tempo real (BARION, 2011).

Na Figura 1, observa-se um modelo do equipamento *MikroTik*, a RB750r2 (*HEX Lite*).

**Figura 1 -** Equipamento MikroTik. **Fonte:** (MIKROTIK, 2019)

## MATERIAL E MÉTODOS

A metodologia utilizada no desenvolvimento desse projeto tem início com uma pesquisa bibliográfica realizada a partir de artigos publicados em eventos, teses, dissertações, monografias, livros, relatórios, periódicos

da área, dentre outros tipos de produções acadêmicas.

Essa pesquisa consiste no levantamento de informações sobre segurança e gerenciamento de redes de computadores.

Após o embasamento teórico, será realizado um levantamento e análise dos principais trabalhos publicados na área de segurança e gerenciamento de redes, destacando os trabalhos que estejam relacionados com o processo de instalação e montagem desse tipo de infraestrutura.

Em seguida, será feito um levantamento e estudo de equipamentos (*hardwares*) e *softwares* que poderão ser utilizados na implantação da rede.

Após esse levantamento, será modelada uma topologia de rede contemplando os aspectos de gerenciamento, qualidade de serviços e segurança estudados.

Com a topologia pronta serão realizadas implementações física e lógica da rede, além da análise do tráfego e da implementação da segurança e do gerenciamento.

Dessa forma, poderá ser observado se a topologia da rede proposta contempla os requisitos mínimos de segurança, *QoS* e gerenciamento.

Durante a execução do projeto, será destinado um tempo para a elaboração dos relatórios: parcial e final, além da escrita e submissão de artigos científicos, para revistas/jornais e eventos, tais como: congressos, seminários, workshop, dentre outros.

Por fim, será elaborado uma *checklist* com os procedimentos necessários para a instalação e configuração de um sistema de gerenciamento e de segurança de redes utilizando uma solução *MikroTik*, que possa servir de guia para futuras instalações e configuração desse tipo de infraestrutura de rede.

## RESULTADOS E DISCUSSÃO

O referido projeto encontra-se em fase de desenvolvimento.

Vale ressaltar, que as fases de levantamento bibliográfico e aquisição de materiais para o projeto já foram concluídas.

No momento, o aluno bolsista encontra-se dedicado ao aprendizado da solução *Mikrotik*, efetuando as instalações e configurações dos equipamentos, para posteriormente efetuar os testes de toda a solução proposta.

Por fim, após as configurações testes, será elaborado uma *checklist* contendo todos os procedimentos necessários para a instalação e configuração de um sistema de gerenciamento e de segurança de redes utilizando uma solução *MikroTik*.

## CONCLUSÕES

O projeto encontra-se em desenvolvimento, e espera-se que o mesmo possa contribuir de forma efetiva para o aprendizado dos envolvidos, em especial do aluno bolsista, fortalecendo o desenvolvimento tecnológico e o conhecimento na área de redes de computadores. Além disso, espera-se que o projeto possa contribuir também para o melhoramento das futuras instalações e configurações de redes de computadores, principalmente em redes que utilizem soluções *MikroTik* na sua infraestrutura.

## REFERÊNCIAS

BARION, Rogério. **Livro MikroTik – Network Associate.** O manual técnico passo a passo. Rio Grande do Sul. Sul Editora, 2011.

CERT.BR. **Cartilha de Segurança para Internet - CERT.br**. Disponível em:https://cartilha.cert.br/. Acesso em: 28 Nov. 2019.

KUROSE, J. F; ROSS, K. W. **Redes de Computadores e a internet**. 3 Ed. São paulo: março de 2009.

MIKROTIK. **MIKROTIK - Produtos**. Disponível em: https://mikrotik.com/product/RB750r2. Acesso em: 28 Nov. 2019.

NAKAMURA, Emílio. Tissato; GEUS, Paulo. Lício. **Segurança de redes em ambientes cooperativos**. 3 Ed. São paulo, 2002.

TORRES, Gabriel. **Redes de Computadores: versão revisada e atualizada**. Rio de Janeiro: Nova Terra, 2009.

TANEMBAUM, Andrew. Stuart. **Computer Network**. 4 Ed, 2003.