**Centro Universitário Estácio de Ribeirão Preto**

Diogo Junior Onofre, 202402655914

Breno Henrique Ninin, 202403018144

Gabriel Baptista Moreira dos Santos, 202403852497

João Pedro Borges Martins, 202403043092

Tiago Rodrigo Ferreira Crippa, 202402349856

Cauã Victor de Souza Santana de Paula, 202402349643

**Estratégias de Defesa Cibernética Baseadas em Análise Preditiva**

Relatório Técnico de Fundamento de Redes

Ribeirão Preto

2024

**Centro Universitário Estácio de Ribeirão Preto**

Diogo Junior Onofre, 202402655914

Breno Henrique Ninin, 202403018144

Gabriel Baptista Moreira dos Santos, 202403852497

João Pedro Borges Martins, 202403043092

Tiago Rodrigo Ferreira Crippa, 202402349856

Cauã Victor de Souza Santana de Paula, 202402349643

**Estratégias de Defesa Cibernética Baseadas em Análise Preditiva**

Relatório Técnico de Fundamento de Redes

Relatório apresentado como requisito avaliativo para a disciplina de Redes de Computadores, do curso de Ciências da Computação, ministrada pelo Prof. Me. Gessé Pereira Evangelista. O objetivo do relatório é permitir que os alunos desenvolvam uma pesquisa focada no estudo de defesa cibernética.

Ribeirão Preto

2024

**Sumário**

[Introdução 4](#_Toc167367480)

[Detecção de Ameaças: 5](#_Toc167367481)

[Prevenção: 7](#_Toc167367482)

[Gerenciamento de Vulnerabilidades: 8](#_Toc167367483)

[Resposta a Incidentes: 10](#_Toc167367484)

[Segurança de Redes: 11](#_Toc167367485)

[Proteção de Dados: 12](#_Toc167367486)

[Comportamento de Usuários: 13](#_Toc167367487)

[Conclusão: 14](#_Toc167367488)

[Referencias Bibliograficas: 15](#_Toc167367489)

# Introdução

Com o avanço na tecnologia e a digitalização das informações, a segurança no tratamento de dados tornou-se urgente, pois a ausência de planejamento pode resultar em danos aos ativos da empresa e comprometimento de dados sensíveis de usuários e colaboradores. Os sistemas de segurança devem ser implementados e monitorados para garantir a segurança do ambiente e dos indivíduos presentes nele, seja esta segurança física ou digital. Para dados e a internet como um todo, é necessário que a segurança na internet receba mais atenção .

A internet, definida como “um conjunto de computadores interconectados para compartilhar informação” , depende fortemente de protocolos que padronizam os dados e garantem parte da segurança. No modelo TCP/IP e suas camadas, é crucial abordar os principais protocolos e como é possível realizar a segurança preditiva.

Considerando os dados transmitidos por este modelo, é importante ressaltar os três pilares da segurança da informação: confidencialidade, integridade e disponibilidade. Para evitar possíveis prejuízos, é necessário utilizar a análise preditiva na segurança da informação, conhecida como segurança preditiva. A segurança preditiva busca prever possíveis eventos futuros com base em dados e algoritmos fornecidos. Para isso, utiliza-se dados e algoritmos de eventos passados para prever acontecimentos que possam oferecer risco ao ambiente monitorado.

Esses dados são como os pacotes de rede ou logs de eventos coletados durante a navegação na web. Sozinhos, esses dados não fornecem insights claros sobre a segurança da rede. No entanto, quando processados e analisados, transformam-se em informação. A partir dessa informação, resultante de um ataque ou de pesquisas e testes, os profissionais de segurança podem implementar medidas adequadas para proteger os sistemas contra ameaças, demonstrando a importância de distinguir entre dados brutos e informações úteis na cibersegurança.

Os ataques que visam o "protocolo de comunicação padrão de todos os navegadores", como o HTTP/HTTPS, se enquadram principalmente na camada de aplicação do modelo TCP/IP. Baseado nas camadas do modelo TCP/IP, existem diferentes tipos de ataques e modos de proteção e é isso que este trabalho irá tratar.

# Detecção de Ameaças:

A detecção de ameaças envolve identificar atividades suspeitas ou maliciosas em sistemas e redes. Isso é feito por meio de ferramentas de monitoramento que analisam o tráfego de rede, logs de eventos e padrões de comportamento.

Os tipos mais comuns de ataques cibernéticos são fundamentais para identificar e responder efetivamente a essas ameaças. Tendo em vista camada de internet (TCP/IP), os ataques mais comuns são:

1. **Camada de Aplicação (TCP/IP)**

**HTTP:**

É o proltocolo de comunicação padrão de todos os navegadores, os ataques que envolvem este protocolo, mais comuns são:

Session hijacking (sequestro de sessão): No hijacking, geralmente, usa-se um sniffer para obter os identificadores (geralmente cookies) e roubar a sessão. Desta forma, é possível que o invasor se passe pelo usuário legítimo e obtenha um aceso não autorizado a uma sessão WEB. Com este acesso não autorizado, é possível se passar pelo usuário e obter dados sensíveis. Ele afeta a integridade do usuário alvo.

Caching: O caching é uma técnica usada para melhorar o desempenho de páginas web, salvando temporariamente cópias de recursos dos dados frequentemente usados. Pórem é possível acessar a máquina do usuário e acessar informações sensíveis por meio dos dados que foram salvos pelo caching

Cookie poisoning (envenenamento de cookies): Os cookies são criados para armazenar informações que possivelmente seráo úteis depois para o site. O armazenamento deles é realizado no computador do usuário. Cookie poisoning é a alteração ou roubo dos cookies do usuário em seu desktop.

Replay attack (ataque de repetição): O replay ataque geralmente funciona com um "man-in-the-middle". Com a interceptação não autorizada dos dados de um servidor, há a repetição de dados, em que o homem no meio acessa o servidor com os dados que pegou e altera a relação dos dados do usuário (seja com transações financeiras, alteração de senha etc).

Cross-site Scripting (XSS): O ataque visa aproveitar de brechas do site para injetar códigos maliciosos, que depois é executado pelo usuário, quando a aplicação modificada é acessada. Desta forma, o hacker pode roubar ou sequestrar e conta.

**Domain name system (DNS):**

O DNS é usado para traduzir nomes de domínios para IP. O problema ocorre quando um hacker direciona o trafego de um site para um servidor errado. Os ataques mais comuns são:

DNS cache poisoning: Inserção de dados falsificados. A informação modificada vai levar para um endereço IP errado e levar a um site falso.

DNS spoofing: Usa um falso IP para combinar com o IP do servidor DNS. A solicitação do usuário vai ser direcionada ao computador do hacker. Neste ataque, o cliente e outros servidores vão considerar o hacker como um servidor DNS.

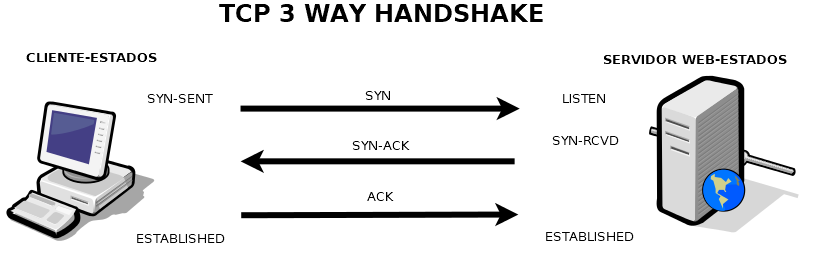
DNS ID hijacking: O mais comum é pela instalação de um malware no computador do usuário que muda o DNS. Este ataque muda o pretador de serviço DNS padrão para algo que o cibercriminoso queira.

1. **Camada de Transporte (TCP/IP)**

**TCP:**

É um protocolo de alta confiança, ele garante que a data chegue com segurança e completa no destino. Este protocolo, ao contrário do UDP, considera que segurança é melhor que velocidade e sempre prioriza que a informação chegue no destinatário.

TCP "SYN" attack: Este ataque quando um cliente manda um pedido de sincronização (para iniciar a conxão) para o servidor, e o servidor manda de volta a sincronização e reserva recursos para a conexão. Neste momento, o cliente deveria mandar um com um pacote ACK (acknowledge) para completar a conexão, mas, no caso do hacker, são enviados vários pacotes SYN, e nenhum pacote ACK é mandado de volta. Resultando na negação do serviço, já que o servidor fica cheio de solicitações sem resposta e torna-se incapaz de responder a outras solicitações.

Figura 1: demonstração do funcionamento do SYN-ACK. Também conhecido como "handshake de 3 vias"

TCP land attack: Ocorre quando o hacker se passa por uma pessoa autorizada (falsifica o IP de origem). A partir disso, o ataque segue similar ao TCP SYN attack

TCP & UDP, port scanning technique: É uma análise do hacker para achar um port disponível na máquina. ports (portar) abertas podem indicar serviços em execução que podem ser explorados por vulnerabilidades. A varredura pode ser feita em portas TCP e UDP.

TCP sequence number prediction: Todos os pacotes enviados entre cliente e servidor tem um número de sequência, o cliente e o servidor trocam a sequência. Neste caso, o hacker preve um número de sequência para se passar por uma pessoa autorizada, e tenta mandar pacotes após se passar pelo IP da vítima.

IP half scan attack: SYN-scanner ou IP half scanning. O atacante envia um pacote SYN, o servidor responde com o SYN/ACK e então o hacker envia um pacote RSC(reset) para fechar a conexão imediatamente. Então, ele registra quais portas responderam com SYN/ACK e quais não responderam

TCP sequence number generation attack: A parte mais importante no TCP é a sequência de números que é trocada entre o usuário e o servidor no início da conexão. UM dos problemas de segurança é a predição do número sequencial, sem receber a resposta do servidor.

1. **Camada de Internet (TCP/IP)**

**IP:**

A principal função do IP é o endereçamento, roteamento e transmissão de pacotes pela internet.

IP spoofing attack: Atacante falsifica o endereço IP de um dos pacotes de origem, fazendo com que os pacoter foram enviados de uma fonte confiável

HTTP flooding: Tipo de ataque DDoS, o hacker sobrecarrega um site com solicitações

Password brute-force attempts: Ataques de força bruta, que tentam advinhar a senha a força, tentativa e erro

Web scraping/data harvesting by competitors:Extração automatizada de dados de um site

Click jacking: Técnica para fazer o usuário clicar em algo diferente do que ele pensa/mostra, geralmente, para isto ocorrer, é usada alguma estratégia de phishing para atrair o cliente à apertar em algum link/botão que foi alterado.

**APR:**

A principal função é estabelecer uma conexão e traduzir da camada da internet para a camada de acesso a rede, de endereços IP a endereços MAC.

Connect hijacking and interception: Sequestro e interceptação de conexões.

Connection reseating: Interrupção de uma conexão TCP existente.

Packet sniff (sniffer): Captura de dados em uma rede.

Denial of service: Negação de serviço, tornando-o inacessível.

Distributed Denial of Service (DDoS): Negação de serviço distribuída, é igual a negação de serviço citada acima, porém para diversos “alvos”.

**IGMP (Internet Group Management Protocol):**

A principal função do IGMP é facilitar a comunicação entre hosts e roteadores multicast.

Multicast Routing: Ataques relacionados ao roteamento de pacotes multicast.

ICMP (Internet Control Message Protocol)

ICMP Tunnelling: Usa pacotes ICMP para encapsular outros tipos de dados, disfarçar a comunicação.

Smurf Attack: Usa mensagens ICMP para sobrecarregar uma rede.

Fraggle Attack: Usa pacotes UDP no lugar de ICMP para realizar o ataque.

# Prevenção:

**Camada de Aplicação**

Session Hijacking (Sequestro de Sessão): O atacante obtém os identificadores de sessão (geralmente cookies) e rouba a sessão, permitindo acesso não autorizado a uma sessão web.

Caching: Técnica usada para melhorar o desempenho de páginas web, salvando temporariamente cópias de recursos de dados frequentemente usados. Pode expor informações sensíveis se o cache for acessado por alguém não autorizado.

Cookie Poisoning (Envenenamento de Cookies): Alteração ou roubo dos cookies do usuário em seu dispositivo.

**Camada de Transporte**

Replay Attack (Ataque de Repetição): O atacante intercepta dados do servidor e os reenvia, permitindo acesso não autorizado a transações ou alterações de dados do usuário.

**Camada de Rede**

Cross-Site Scripting (XSS): Aproveita brechas no site para injetar códigos maliciosos que serão executados pelo usuário.

Domain Name System (DNS):

DNS Cache Poisoning: Inserção de dados falsificados no cache DNS, direcionando os usuários para um site falso.

DNS Spoofing: Uso de um falso IP para combinar com o IP do servidor DNS, direcionando as solicitações do usuário para o computador do hacker.

DNS ID Hijacking: Alteração do provedor de serviço DNS padrão para um desejado pelo cibercriminoso, geralmente através de malware.

# Gerenciamento de Vulnerabilidades:

O gerenciamento de vulnerabilidades é um processo essencial dentro da camada de segurança de qualquer organização. Ele envolve a identificação, avaliação, tratamento e monitoramento contínuo de vulnerabilidades em sistemas, redes e aplicações. Aqui está uma visão geral detalhada das etapas principais do gerenciamento de vulnerabilidades:

1. **Identificação de Vulnerabilidades**

Esta etapa envolve a detecção de vulnerabilidades conhecidas e desconhecidas em sistemas e aplicações. As ferramentas e técnicas comuns incluem:

Scanners de vulnerabilidades: Ferramentas como Nessus, Qualys e OpenVAS que realizam varreduras automáticas em redes e sistemas para identificar pontos fracos conhecidos.

Análise de código estático e dinâmico: Inspeção de código-fonte para identificar vulnerabilidades de software.

Testes de penetração (Pentests): Simulações controladas de ataques para identificar vulnerabilidades exploráveis.

1. **Avaliação de Vulnerabilidades**

Depois de identificadas, as vulnerabilidades precisam ser avaliadas quanto ao seu impacto e à probabilidade de exploração. Isso ajuda a priorizar as ações corretivas. As atividades nesta fase incluem:

Classificação de risco: Usar sistemas de pontuação como CVSS (Common Vulnerability Scoring System) para avaliar a gravidade de cada vulnerabilidade.

Análise de impacto: Avaliar o impacto potencial sobre os ativos críticos da organização caso a vulnerabilidade seja explorada.

1. **Tratamento de Vulnerabilidades**

O tratamento envolve a mitigação, remediação ou aceitação do risco associado a uma vulnerabilidade. As opções incluem:

Aplicação de patches: Atualizar softwares e sistemas com patches fornecidos pelos fornecedores.

Configurações de segurança: Ajustar configurações para reduzir a exposição, como desabilitar serviços desnecessários ou modificar permissões.

Medidas compensatórias: Implementar controles adicionais como firewalls, sistemas de detecção de intrusão (IDS) ou redes segmentadas para limitar o impacto.

1. **Monitoramento Contínuo**

A segurança é um processo contínuo e dinâmico. O monitoramento contínuo é essencial para

Reavaliar vulnerabilidades: Garantir que as vulnerabilidades sejam tratadas e que novas vulnerabilidades não apareçam.

Relatórios regulares: Manter registros e relatórios de vulnerabilidades para auditorias e conformidade.

Alertas e notificações: Utilizar sistemas que fornecem alertas em tempo real sobre novas vulnerabilidades e ameaças emergentes.

1. **Ferramentas e Tecnologias Utilizadas**

Diversas ferramentas e tecnologias podem ser empregadas no gerenciamento de vulnerabilidades:

Sistemas de Gerenciamento de Vulnerabilidades (VMS): Soluções integradas que automatizam a identificação, avaliação e tratamento de vulnerabilidades.

Sistemas de Detecção e Prevenção de Intrusões (IDS/IPS): Detectam e previnem tentativas de exploração de vulnerabilidades.

Firewalls e Gateways de Segurança: Controlam o tráfego de rede para prevenir acesso não autorizado.

1. **Boas Práticas:**

Para um gerenciamento eficaz de vulnerabilidades, é importante seguir algumas boas práticas:

Treinamento contínuo: Garantir que a equipe de segurança esteja sempre atualizada sobre as melhores práticas e novas ameaças.

Gestão de ativos: Manter um inventário atualizado de todos os ativos de TI para facilitar a identificação de vulnerabilidades.

Políticas de segurança: Desenvolver e implementar políticas de segurança claras e abrangentes.

O gerenciamento de vulnerabilidades é um componente crítico da estratégia de segurança cibernética de qualquer organização. Um processo bem estruturada ajuda a identificar e mitigar riscos, proteger ativos valiosos e garantir a conformidade com normas e regulamentos de segurança.

# Resposta a Incidentes:

Antes que um incidente ocorra, é essencial que a organização esteja preparada para responder de maneira eficaz. Isso envolve o desenvolvimento e documentação de políticas de segurança e procedimentos de resposta a incidentes, a formação de uma equipe dedicada e treinada para lidar com incidentes de segurança (Equipe de Resposta a Incidentes - IRT), e a garantia de que as ferramentas necessárias (SIEM, IDS/IPS, antivírus, etc.) estejam instaladas e configuradas corretamente. Além disso, é crucial estabelecer um plano de comunicação claro para informar as partes interessadas durante e após um incidente.

A detecção precoce de incidentes é vital para limitar o impacto. Isso pode ser alcançado através de monitoramento contínuo, utilizando sistemas de monitoramento e logs para detectar atividades suspeitas em todas as camadas (aplicação, transporte, internet e rede). É importante configurar alertas para atividades anômalas ou potenciais incidentes e analisar os dados coletados para confirmar a existência de um incidente e avaliar sua gravidade.

Após a detecção de um incidente, o próximo passo é conter o incidente para limitar os danos e erradicar a causa raiz. Isso envolve isolar sistemas comprometidos para evitar a propagação do incidente, implementar medidas imediatas para mitigar os danos, como bloquear IPs maliciosos ou interromper serviços afetados, e remover a causa raiz do incidente, como malware ou vulnerabilidades exploradas, utilizando ferramentas de remoção de malware e aplicando patches de segurança.

Depois de conter e erradicar o incidente, é necessário restaurar os sistemas e serviços afetados à operação normal. Isso inclui restaurar sistemas a partir de backups limpos, testar os sistemas restaurados para garantir que estejam funcionando corretamente e que não haja vestígios do incidente, e monitorar os sistemas restaurados para detectar qualquer atividade anômala residual.

A fase final de resposta a incidentes envolve a revisão do incidente e a implementação de melhorias para prevenir futuros incidentes. Isso inclui realizar uma análise detalhada do incidente para entender o que aconteceu, como foi detectado, como foi respondido e o que poderia ser melhorado. Todas as ações tomadas durante o incidente e as lições aprendidas devem ser documentadas, e políticas, procedimentos e ferramentas devem ser revisados e atualizados com base nas lições aprendidas. É importante realizar treinamentos baseados nas lições aprendidas para melhorar a resposta a futuros incidentes.

A comunicação eficiente é crítica durante todas as etapas de resposta a incidentes. É necessário manter as partes interessadas informadas sobre o progresso e impacto do incidente e ser transparente com os clientes e reguladores, quando apropriado, sobre a natureza do incidente e as medidas tomadas.

Agora, focando nas camadas TCP/IP, temos:

**Camada de Aplicação**

* Monitoramento de Aplicações: Implementar monitoramento de integridade e segurança nas aplicações críticas.
* Patching Regular: Manter todas as aplicações atualizadas com os patches de segurança mais recentes.

**Camada de Transporte**

* Criptografia de Dados: Garantir que os dados em trânsito estejam protegidos por criptografia adequada.
* Análise de Tráfego: Usar análise de tráfego para detectar padrões anômalos.

**Camada de Internet**

* Segurança de Rede: Implementar firewalls e IDS/IPS para proteger contra ameaças de rede.
* Análise de Risco: Avaliar continuamente os riscos e atualizar as medidas de segurança.

**Camada de Acesso à Rede**

* Controles de Acesso: Garantir que apenas dispositivos e usuários autorizados possam acessar a rede.
* Monitoramento de Dispositivos: Monitorar dispositivos de rede para alterações não autorizadas.

# Segurança de Redes:

A segurança da rede é um aspecto fundamental na proteção das informações e dos sistemas dentro de uma organização. Para garantir a integridade, a confidencialidade e a disponibilidade dos dados, é necessário implementar medidas de segurança em todas as camadas da rede. Vamos explorar as principais camadas de uma rede e as práticas recomendadas de segurança para cada uma delas.

**1. Camada Física**

**Descrição:** A camada física refere-se aos componentes de hardware da rede, como cabos, switches, roteadores e dispositivos de rede.

**Medidas de Segurança:**

* **Controle de Acesso Físico:** Restrição de acesso a salas de servidores e equipamentos de rede através de chaves, cartões de acesso ou biometria.
* **Monitoramento e Vigilância:** Uso de câmeras de segurança e sistemas de vigilância para monitorar atividades suspeitas nas áreas onde os equipamentos estão localizados.
* **Proteção contra Desastres:** Implementação de medidas de proteção contra incêndios, inundações e outras ameaças físicas, além de garantir a redundância e o backup dos sistemas.

**2. Camada de Enlace**

**Descrição:** A camada de enlace é responsável pela transferência de dados entre dispositivos na mesma rede local (LAN). Envolve protocolos como Ethernet e Wi-Fi.

**Medidas de Segurança:**

* **Filtragem de MAC:** Limitação do acesso à rede a dispositivos com endereços MAC específicos para evitar conexões não autorizadas.
* **Criptografia de Tráfego:** Uso de protocolos como WPA3 para criptografar o tráfego de rede Wi-Fi e proteger contra eavesdropping.
* **Segmentação de Rede:** Criação de VLANs (Redes Locais Virtuais) para isolar diferentes segmentos de rede e limitar a propagação de ataques.

**3. Camada de Rede**

**Descrição:** A camada de rede gerencia o roteamento dos pacotes de dados entre diferentes redes. Protocolos como IP (Internet Protocol) operam nesta camada.

**Medidas de Segurança:**

* **Firewall:** Implementação de firewalls para filtrar tráfego malicioso e controlar o acesso entre redes internas e externas.
* **Sistemas de Prevenção de Intrusão (IPS):** Utilização de IPS para detectar e bloquear atividades suspeitas e ataques.
* **VPN (Rede Privada Virtual):** Uso de VPNs para criar conexões seguras e criptografadas entre dispositivos remotos e a rede corporativa.

**4. Camada de Transporte**

**Descrição:** A camada de transporte garante a transferência confiável de dados entre sistemas. Protocolos como TCP (Transmission Control Protocol) e UDP (User Datagram Protocol) funcionam nesta camada.

**Medidas de Segurança:**

* **TLS (Transport Layer Security):** Implementação de TLS para criptografar dados em trânsito e garantir a comunicação segura entre clientes e servidores.
* **Gestão de Sessões:** Monitoramento e gerenciamento de sessões para identificar e interromper conexões suspeitas.
* **Filtragem de Portas:** Configuração de firewalls para bloquear portas não utilizadas e potencialmente vulneráveis.

**5. Camada de Aplicação**

**Descrição:** A camada de aplicação é onde os aplicativos e os serviços de rede, como HTTP, FTP e SMTP, interagem com os usuários.

**Medidas de Segurança:**

* **Autenticação e Autorização:** Implementação de métodos robustos de autenticação (senhas fortes, autenticação multifator) e controle de acesso baseado em funções.
* **Firewalls de Aplicação Web (WAF):** Uso de WAFs para proteger aplicativos web contra ataques comuns como SQL injection e cross-site scripting (XSS).
* **Análise de Vulnerabilidades:** Realização de testes regulares de penetração e análise de vulnerabilidades para identificar e corrigir falhas de segurança nos aplicativos.

A segurança da rede dessa forma requer uma abordagem abrangente que abrange todas as camadas do modelo OSI. Cada camada tem suas próprias vulnerabilidades e requer medidas de segurança específicas para proteger contra ameaças potenciais. Ao implementar essas práticas de segurança de forma integrada, as organizações podem proteger melhor seus dados e sistemas contra uma ampla gama de ataques e ameaças cibernéticas.

# Proteção de Dados:

A proteção de dados na camada física envolve várias medidas de segurança para proteger os equipamentos e meios físicos onde os dados são armazenados e transmitidos. Aqui estão as principais estratégias usadas:

**Controle de Acesso Físico:**

Isso inclui restringir quem pode entrar em áreas onde estão localizados servidores e outros equipamentos críticos, utilizando sistemas como cartões de identificação e biometria para verificar quem entra.

**Monitoramento e Vigilância:**

Usar câmeras de segurança para monitorar áreas sensíveis e ter equipes de segurança que fazem rondas regulares para garantir que tudo está em ordem.

**Proteção contra Desastres:**

Instalar sistemas de detecção e supressão de incêndios, e manter o ambiente com temperatura e umidade controladas para proteger os equipamentos.

**Segurança dos Equipamentos:**

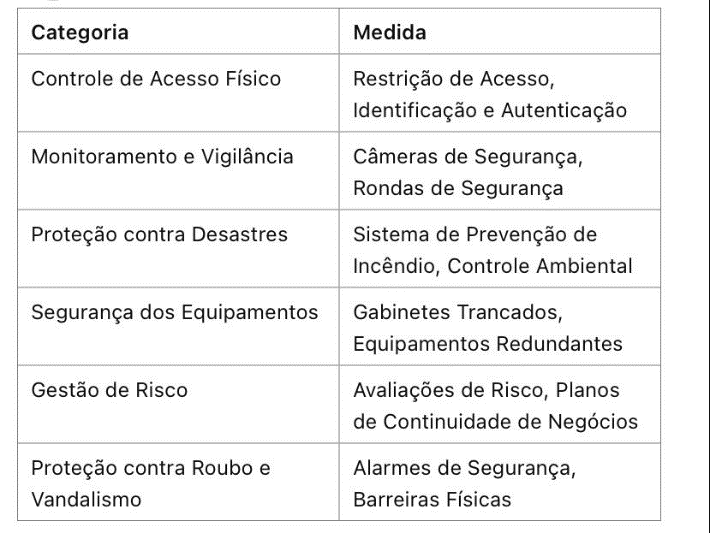
Manter servidores e outros dispositivos em racks trancados para prevenir acessos não autorizados, e usar fontes de energia ininterrupta (UPS) e geradores para garantir que tudo continue funcionando mesmo em caso de falha de energia.

**Gestão de Risco:**

Realizar avaliações regulares para identificar possíveis ameaças à segurança física e ter planos de recuperação de desastres para garantir que os dados possam ser recuperados se algo der errado.

**Proteção contra Roubo e Vandalismo:**

Instalar alarmes de segurança e construir barreiras físicas como cercas e muros para dificultar o acesso não autorizado.



# Comportamento de Usuários:

Baseado nas camadas do protocolo TCP/IP, temos:

**Camada de aplicação:**

* Interação com diversos serviços como web browsers, emails, redes sociais e aplicativos de mensagens.
* Escolha de senhas, configuração de perfis de privacidade.

**Camada de Transporte:**

* Escolha de protocolos como TCP ou UDP
* Expectativas do usuário em relação à latência, largura de banda e estabilidade da conexão.

**Camada de Rede:**

* Uso de VPNs para proteger sua privacidade e dados online, especialmente quando se conectam a redes públicas ou não confiáveis.
* Usuários podem ser afetados por ameaças na camada de rede, como ataques DDoS (Distributed Denial of Service), que visam sobrecarregar a rede e tornála indisponível.

# Conclusão:

É essencial compreender as diferentes camadas do modelo TCP/IP e os tipos de ataques associados a cada uma delas para implementar uma defesa eficaz.

Na Camada de Aplicação, onde os protocolos como HTTP, HTTPS, FTP, SMTP e DNS são predominantes, enfrentamos ataques como SQL Injection, CrossSite Scripting (XSS), CrossSite Request Forgery (CSRF), Phishing e ManintheMiddle (MitM). Esses ataques visam diretamente as interfaces e os protocolos que as aplicações utilizam para se comunicar, tornando crucial a implementação de medidas robustas de segurança nessa camada.

A Camada de Transporte é responsável pela comunicação de dados fim a fim entre dispositivos, utilizando protocolos como TCP e UDP. Ataques como SYN Flood e UDP Flood têm como objetivo sobrecarregar os servidores e esgotar recursos, exigindo estratégias de mitigação específicas para proteger a integridade e a disponibilidade dos serviços.

Na Camada de Internet, os protocolos IP e ICMP são utilizados para a movimentação dos pacotes de dados através da rede. Ataques de IP Spoofing e ICMP Flood são comuns nesta camada, podendo comprometer a confiabilidade das comunicações de rede. A proteção contra esses tipos de ataques é vital para garantir a integridade e a continuidade das operações de rede.

Por fim, a Camada de Acesso à Rede envolve tecnologias de enlace de dados e física como Ethernet e WiFi. Ataques de MAC Spoofing e ARP Spoofing podem redirecionar o tráfego de rede e comprometer a segurança dos dados transmitidos. A implementação de medidas de segurança nesta camada é essencial para proteger contra acessos não autorizados e garantir a confidencialidade dos dados.

A análise preditiva emerge como uma ferramenta fundamental na cibersegurança, pois permite prever e mitigar ameaças futuras com base em dados e algoritmos derivados de eventos passados. Utilizando sistemas de segurança preditiva, as organizações podem identificar padrões de ataque, antecipar possíveis vulnerabilidades e implementar medidas preventivas antes que ocorram incidentes.

Dessa forma, uma abordagem abrangente de segurança da informação que abrange todas as camadas do modelo TCP/IP, aliada à análise preditiva, é crucial para proteger contra a ampla gama de ameaças cibernéticas e assegurar a integridade, confidencialidade e disponibilidade dos dados e sistemas.

# REFERENCIAS BIBLIOGRÁFICAS:

**[1]NAZ, SAMINA** & **PARVEEN, ZAHIDA** & **ALRASHIDI, BEDOUR.** Security issues of TCP/IP model at layers levels. Disponível em: <https://www.researchgate.net/publication/330132778_Security_issues_in_Protocols_of_TCPIP_Model_at_Layers_Level>.

**CISCO**. O que é segurança de rede. Disponível em: <https://www.cisco.com/c/pt\_br/products/security/what-is-network-security.html>. Acesso em: 10 maio 2024.

**REVISTA SEGURANÇA ELETRÔNICA.** Análise preditiva ganha destaque em meio à onda de ciberataques. Disponível em: <https://revistasegurancaeletronica.com.br/analise-preditiva-ganha-destaque-em-meio-a-onda-de-ciberataques/>. Acesso em: 10 maio 2024.

**ISH.** Cibersegurança e a inteligência artificial. Disponível em: <https://www.ish.com.br/blog/ciberseguranca-e-a-inteligencia-artificial/#:~:text=Atrav%C3%A9s%20da%20an%C3%A1lise%20preditiva%2C%20sistemas,a%20seguran%C3%A7a%20das%20infraestruturas%20digitais>. Acesso em: 10 maio 2024.

**AVANTIA.** O que são sistemas de segurança preditivos. Disponível em: <https://www.avantia.com.br/blog/o-que-sao-sistemas-de-seguranca-preditivos/>. Acesso em: 10 maio 2024.

**GOOGLE CLOUD.** O que é análise preditiva? Disponível em: <https://cloud.google.com/learn/what-is-predictive-analytics?hl=pt-br>. Acesso em: 10 maio 2024.

**TECHTARGET.** Port number. Disponível em: <https://www.techtarget.com/searchnetworking/definition/port-number>. Acesso em: 10 maio 2024.

**GLOBALSIGN.** Session hijacking and how to prevent it. Disponível em: <https://www.globalsign.com/en/blog/session-hijacking-and-how-to-prevent-it>. Acesso em: 10 maio 2024.

**ESECURITY PLANET.** How to prevent DNS attacks. Disponível em: <https://www.esecurityplanet.com/networks/how-to-prevent-dns-attacks/>. Acesso em: 10 maio 2024.

**IT'S ASAP.** How to prevent brute force attacks. Disponível em: <https://www.itsasap.com/blog/how-to-prevent-brute-force-attacks>. Acesso em: 10 maio 2024.

**OKTA.** Fraggle attack. Disponível em: <https://www.okta.com/identity-101/fraggle-attack/>. Acesso em: 10 maio 2024.

**PURPLESEC.** Prevent SYN flood attack. Disponível em: <https://purplesec.us/prevent-syn-flood-attack/>. Acesso em: 10 maio 2024.

**FORTINET.** What is port scan. Disponível em: <https://www.fortinet.com/resources/cyberglossary/what-is-port-scan>. Acesso em: 10 maio 2024.

**LINKEDIN.** How can you prevent TCP sequence number prediction. Disponível em: <https://www.linkedin.com/advice/3/how-can-you-prevent-tcp-sequence-number-prediction>. Acesso em: 10 maio 2024.

**GOCACHE**. O que é modelo OSI, seus ataques e como se proteger. Disponível em: <https://www.google.com/amp/s/www.gocache.com.br/seguranca/o-que-e-modelo-osi-seus-ataques-e-como-se-proteger/amp/>. Acesso em: 10 maio 2024.