# INTRODUÇÃO A SEGURANÇA DE REDES 1.0

JOAS ANTONIO

# SOBRE O LIVRO

- Conceitos básicos de redes e segurança de redes de computadores;
- Um livro básico para iniciantes na área de segurança;
- Baseado em conteúdos de certificações;
- Um livro teórico que contém apenas conceitos;

# SOBRE O AUTOR

- Nome: Joas Antonio;
- Entusiasta e apaixonado por Segurança da Informação;
- Apenas gosto de escrever e contribuir com a comunidade de segurança da informação;

# CONCEITOS DE REDES DE COMPUTADORES

# O QUE É REDES DE COMPUTADORES?

- Uma rede de computadores é um grupo de sistemas de computadores e outros dispositivos de hardware de computação que estão ligados entre si através de canais de comunicação para facilitar a comunicação e o compartilhamento de recursos entre uma ampla gama de usuários. Redes são geralmente classificadas com base em suas características.
- Um dos primeiros exemplos de uma rede de computadores foi uma rede de comunicação de computadores que funcionavam como parte do sistema de radar do exército norte-americano. Em 1969, a Universidade da Califórnia em Los Angeles, o Stanford Research Institute, da Universidade da Califórnia em Santa Barbara e a Universidade de Utah foram conectadas como parte do projeto Advanced Research Projects Agency Network (ARPANET). É esta rede que evoluiu para se tornar o que hoje conhecemos simplesmente pelo nome de Internet.

# O QUE É REDES DE COMPUTADORES?

- As redes são usadas para:
- Facilitar a comunicação via e-mail, videoconferência, mensagens instantâneas etc.
- Permitir que vários usuários compartilhem um único dispositivo de hardware, como uma impressora ou scanner;
- Ativar compartilhamento de arquivos;
- Permitir a partilha de programas de software ou de funcionamento em sistemas remotos;
- Tornar a informação mais fácil de acessar e manter entre vários usuários num mesmo ambiente ou em ambientes distintos (com acesso remoto, via web, por exemplo).

# TIPOS DE REDES DE COMPUTADORES

**1. Rede de Área Pessoal (PAN)**

- O menor e mais básico tipo de rede, um PAN é composto de um modem sem fio, um computador ou dois, telefones, impressoras, tablets etc., e gira em torno de uma pessoa em um prédio. Esses tipos de redes geralmente são encontrados em pequenos escritórios ou residências e são gerenciados por uma pessoa ou organização a partir de um único dispositivo.

**2. Rede Local (LAN)**

- Estamos confiantes de que você já ouviu falar desses tipos de redes antes - as LANs são as redes mais discutidas, uma das mais comuns, uma das mais originais e uma das mais simples. As LANs conectam grupos de computadores e dispositivos de baixa tensão em distâncias curtas (dentro de um edifício ou entre um grupo de dois ou três edifícios próximos um do outro) para compartilhar informações e recursos. As empresas geralmente gerenciam e mantêm LANs.
- Usando roteadores, as LANs podem se conectar a redes de longa distância (WANs, explicadas abaixo) para transferir dados com rapidez e segurança.

# TIPOS DE REDES DE COMPUTADORES

**3. Rede local sem fio (WLAN)**

- Funcionando como uma LAN, as WLANs usam tecnologia de rede sem fio , como Wi-Fi. Geralmente vistos nos mesmos tipos de aplicativos que as LANs, esses tipos de redes não exigem que os dispositivos confiem em cabos físicos para se conectar à rede.

**4. Rede de Área do Campus (CAN)**

- Maiores que as LANs, mas menores que as redes de área metropolitana (MANs, explicadas abaixo), esses tipos de redes são normalmente vistos em universidades, grandes distritos escolares do ensino fundamental e médio ou pequenas empresas. Eles podem se espalhar por vários prédios bastante próximos um do outro, para que os usuários possam compartilhar recursos.

# TIPOS DE REDES DE COMPUTADORES

**5. Rede de Área Metropolitana (MAN)**

- Esses tipos de redes são maiores que as LANs, mas menores que as WANs - e incorporam elementos dos dois tipos de redes. Os MANs abrangem uma área geográfica inteira (normalmente uma cidade ou cidade, mas às vezes um campus). A propriedade e a manutenção são gerenciadas por uma única pessoa ou empresa (um conselho local, uma grande empresa etc.).

**6. Rede de Área Ampla (WAN)**

- Um pouco mais complexa que uma LAN, uma WAN conecta computadores juntos por distâncias físicas mais longas. Isso permite que computadores e dispositivos de baixa tensão sejam conectados remotamente uns aos outros através de uma grande rede para se comunicar mesmo quando estão separados por quilômetros.
- A Internet é o exemplo mais básico de uma WAN, conectando todos os computadores ao redor do mundo. Devido ao amplo alcance de uma WAN, ela geralmente pertence e é mantida por vários administradores ou pelo público.

# TIPOS DE REDES DE COMPUTADORES

**7. Rede de Área de Armazenamento (SAN)**

- Como uma rede dedicada de alta velocidade que conecta conjuntos compartilhados de dispositivos de armazenamento a vários servidores, esses tipos de redes não dependem de uma LAN ou WAN. Em vez disso, eles afastam os recursos de armazenamento da rede e os colocam em sua própria rede de alto desempenho. As SANs podem ser acessadas da mesma maneira que uma unidade conectada a um servidor. Os tipos de redes de área de armazenamento incluem SANs convergidas, virtuais e unificadas.

**8. Rede da área do sistema (também conhecida como SAN)**

- Este termo é relativamente novo nas últimas duas décadas. É usado para explicar uma rede relativamente local projetada para fornecer conexão de alta velocidade em aplicativos de servidor para servidor (ambientes em cluster), redes de área de armazenamento (também chamadas de “SANs”) e aplicativos de processador para processador. Os computadores conectados a uma SAN operam como um sistema único em velocidades muito altas.

# TIPOS DE REDES DE COMPUTADORES

**9. Rede óptica local passiva (POLAN)**

- Como alternativa às LANs Ethernet tradicionais baseadas em comutador, a tecnologia POLAN pode ser integrada ao cabeamento estruturado para superar as preocupações sobre o suporte aos protocolos Ethernet tradicionais e aplicativos de rede como PoE (Power over Ethernet). Uma arquitetura de LAN ponto a multiponto, o POLAN usa divisores ópticos para dividir um sinal óptico de um fio de fibra óptica monomodo em vários sinais para atender usuários e dispositivos.

**10. Rede Privada Corporativa (EPN)**

- Esses tipos de redes são criados e pertencem a empresas que desejam conectar com segurança seus vários locais para compartilhar recursos do computador.

**11. Rede Privada Virtual (VPN)**

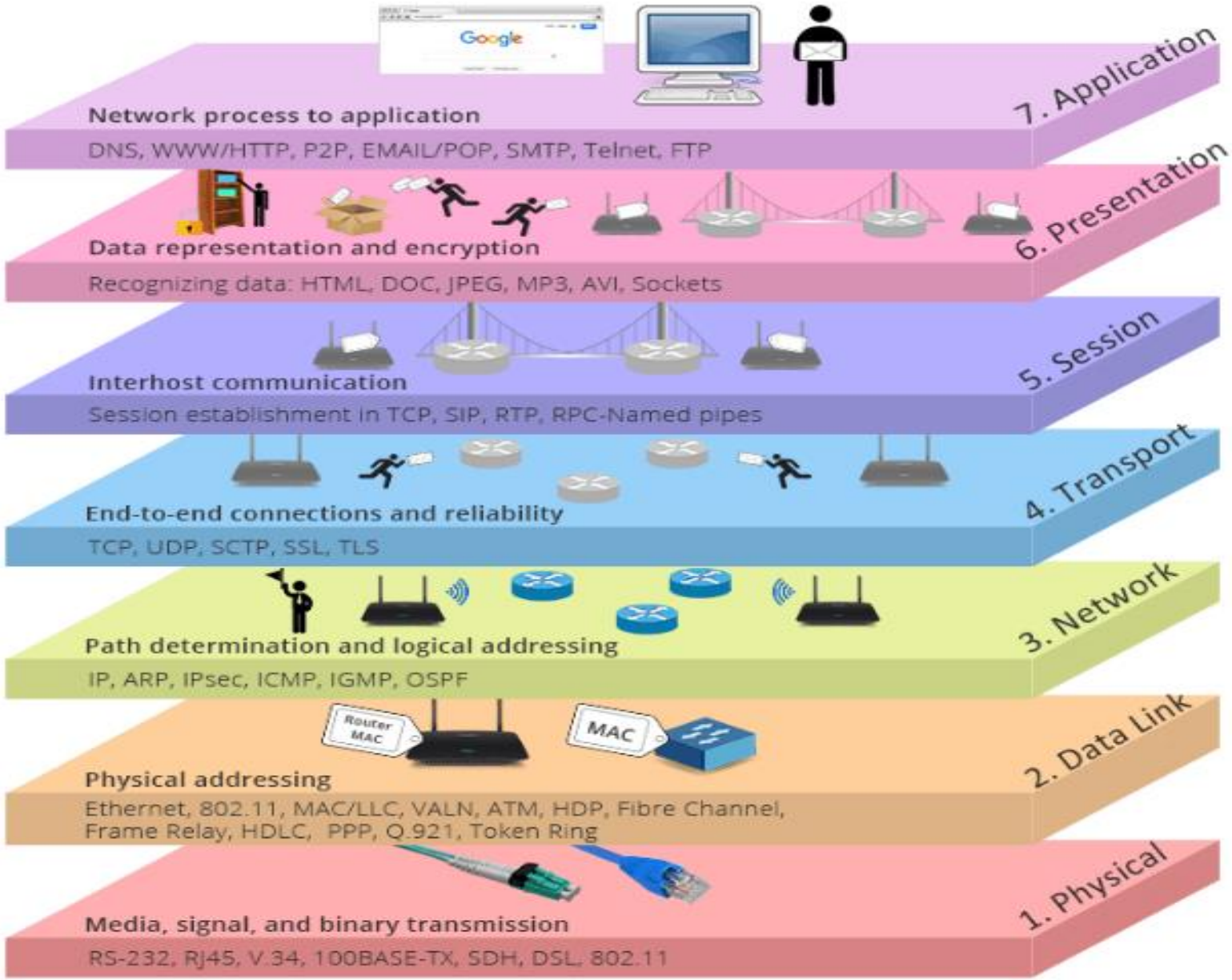
- Ao estender uma rede privada pela Internet, uma VPN permite que seus usuários enviem e recebam dados como se seus dispositivos estivessem conectados à rede privada - mesmo que não estejam. Por meio de uma conexão ponto a ponto virtual, os usuários podem acessar uma rede privada remotamente.

https://www.belden.com/blog/smart-building/network-types

# MODELO OSI

- O modelo Open Systems Interconnection (OSI) é um modelo conceitual criado pela Organização Internacional de Padronização que permite que diversos sistemas de comunicação se comuniquem usando protocolos padrão. Em inglês simples, o OSI fornece um padrão para que diferentes sistemas de computadores possam se comunicar.
- O modelo OSI pode ser visto como uma linguagem universal para redes de computadores. É baseado no conceito de dividir um sistema de comunicação em sete camadas abstratas, cada uma empilhada na última.

# MODELO OSI – REPRESENTAÇÃO EM IMAGEM



# MODELO OSI – REPRESENTAÇÃO EM IMAGEM

**Resumo das Camadas do Modelo OSI**

| | |
|---|---|
| Aplicação | Prover serviços de rede às aplicações |
| Apresentação | Criptografia, codificação, compressão e formatos de dados |
| Sessão | Iniciar, manter e finalizar sessões de comunicação |
| Transporte | Transmissão confiável de dados, segmentação |
| Rede | Endereçamento lógico e roteamento; controle de tráfego |
| Link de Dados | Endereçamento físico; transmissão confiável de quadros |
| Física | Interface com meios de transmissão e sinalização |

# MODELO OSI – 7 CAMADAS

7. A camada de aplicação

- Essa é a única camada que interage diretamente com os dados do usuário. Aplicativos de software, como navegadores da Web e clientes de email, contam com a camada de aplicativos para iniciar as comunicações. Mas deve ficar claro que os aplicativos de software cliente não fazem parte da camada de aplicativo; em vez disso, a camada de aplicação é responsável pelos protocolos e manipulação de dados nos quais o software confia para apresentar dados significativos ao usuário. Os protocolos da camada de aplicativos incluem HTTP e SMTP (o Simple Mail Transfer Protocol é um dos protocolos que permite a comunicação por email).

# MODELO OSI – 7 CAMADAS

6. A camada de apresentação

- Essa camada é responsável principalmente pela preparação dos dados para que possam ser usados pela camada de aplicação; em outras palavras, a camada 6 torna os dados apresentáveis para os aplicativos consumirem. A camada de apresentação é responsável pela tradução, criptografia e compactação de dados.
- Dois dispositivos de comunicação que se comunicam podem estar usando métodos de codificação diferentes; portanto, a camada 6 é responsável por converter os dados recebidos em uma sintaxe que a camada de aplicação do dispositivo receptor pode entender.
- Se os dispositivos estiverem se comunicando através de uma conexão criptografada, a camada 6 é responsável por adicionar a criptografia na extremidade do remetente, bem como decodificar a criptografia na extremidade do receptor, para que ele possa apresentar à camada de aplicação dados legíveis e não criptografados.
- Finalmente, a camada de apresentação também é responsável por compactar os dados que recebe da camada de aplicação antes de entregá-la à camada 5. Isso ajuda a melhorar a velocidade e a eficiência da comunicação, minimizando a quantidade de dados que serão transferidos.

# MODELO OSI – 7 CAMADAS

5. A camada de sessão

- Essa é a camada responsável pela abertura e fechamento da comunicação entre os dois dispositivos. O tempo entre o momento em que a comunicação é aberta e fechada é conhecido como a sessão. A camada da sessão garante que a sessão permaneça aberta por tempo suficiente para transferir todos os dados que estão sendo trocados e feche prontamente a sessão para evitar o desperdício de recursos.
- A camada de sessão também sincroniza a transferência de dados com os pontos de verificação. Por exemplo, se um arquivo de 100 megabytes estiver sendo transferido, a camada da sessão poderá definir um ponto de verificação a cada 5 megabytes. No caso de uma desconexão ou falha após a transferência de 52 megabytes, a sessão pode ser retomada a partir do último ponto de verificação, o que significa que apenas mais 50 megabytes de dados precisam ser transferidos. Sem os pontos de verificação, toda a transferência teria que começar novamente do zero.

# MODELO OSI – 7 CAMADAS

4. A camada de transporte

- A camada 4 é responsável pela comunicação de ponta a ponta entre os dois dispositivos. Isso inclui pegar dados da camada de sessão e dividi-los em pedaços chamados segmentos antes de enviá-los para a camada 3. A camada de transporte no dispositivo receptor é responsável por remontar os segmentos em dados que a camada de sessão pode consumir.
- A camada de transporte também é responsável pelo controle de fluxo e controle de erros. O controle de fluxo determina uma velocidade ótima de transmissão para garantir que um remetente com uma conexão rápida não sobrecarregue um receptor com uma conexão lenta. A camada de transporte executa o controle de erros no lado receptor, garantindo que os dados recebidos sejam completos e solicitando uma retransmissão, se não estiverem.

# MODELO OSI – 7 CAMADAS

3. A camada de rede

- A camada de rede é responsável por facilitar a transferência de dados entre duas redes diferentes. Se os dois dispositivos que estão se comunicando estiverem na mesma rede, a camada de rede será desnecessária. A camada de rede divide os segmentos da camada de transporte em unidades menores, chamadas pacotes, no dispositivo do remetente e remontando esses pacotes no dispositivo receptor. A camada de rede também encontra o melhor caminho físico para os dados chegarem ao seu destino; isso é conhecido como roteamento.

# MODELO OSI – 7 CAMADAS

2. A camada de enlace de dados

- A camada de enlace de dados é muito semelhante à camada de rede, exceto que a camada de enlace de dados facilita a transferência de dados entre dois dispositivos na mesma rede. A camada de enlace de dados pega pacotes da camada de rede e os divide em pedaços menores chamados quadros. Assim como a camada de rede, a camada de enlace de dados também é responsável pelo controle de fluxo e controle de erros na comunicação intra-rede (a camada de transporte apenas faz controle de fluxo e controle de erros para comunicações entre redes).

# MODELO OSI – 7 CAMADAS

1. A camada física

- Essa camada inclui o equipamento físico envolvido na transferência de dados, como cabos e comutadores. Essa também é a camada na qual os dados são convertidos em um fluxo de bits, que é uma sequência de 1s e 0s. A camada física de ambos os dispositivos também deve concordar com uma convenção de sinal, para que os 1s possam ser distinguidos dos 0s em ambos os dispositivos.

- https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/

# MODELO TCP/IP

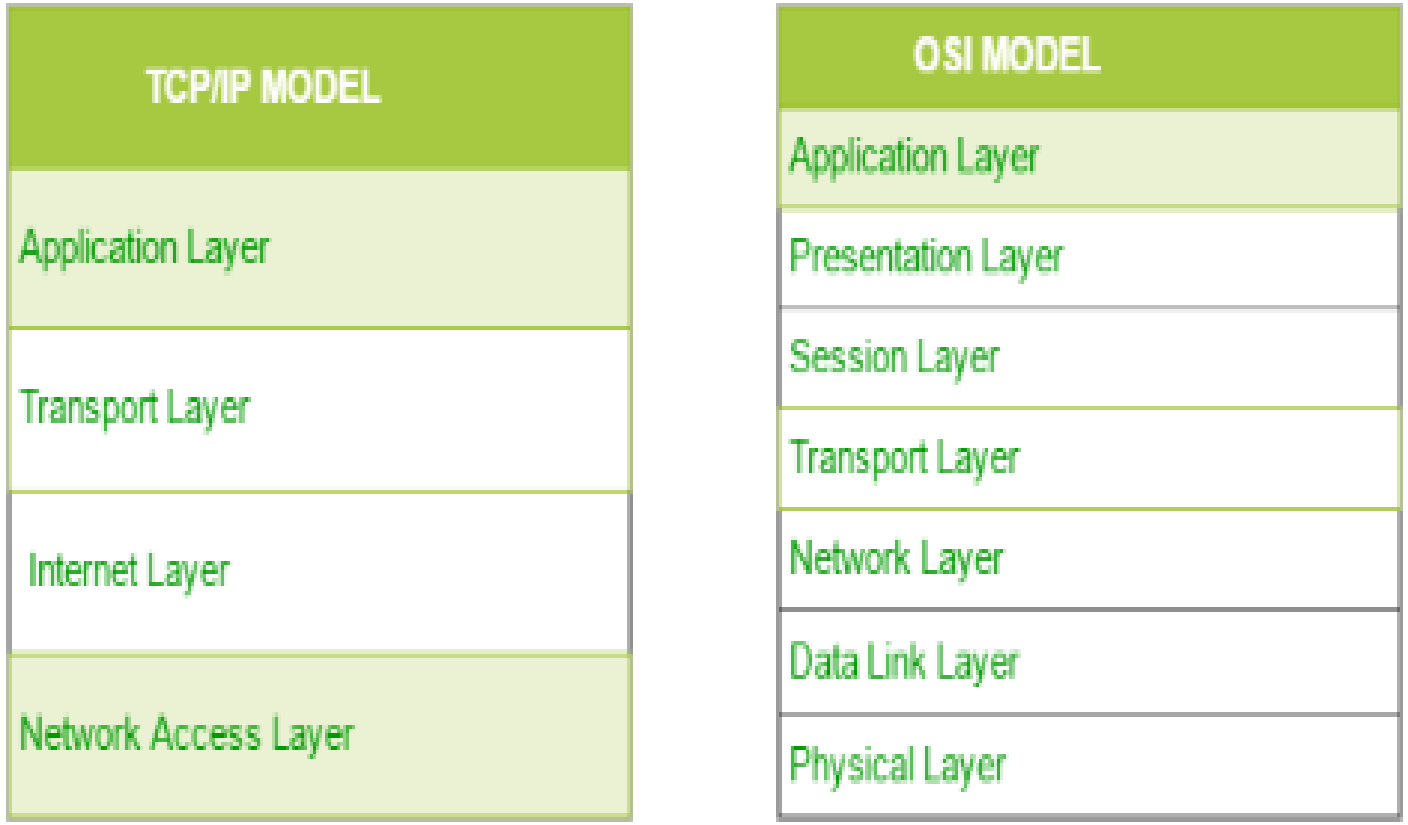
- **O modelo TCP / IP** ajuda a determinar como um computador específico deve ser conectado à Internet e como os dados devem ser transmitidos entre eles. Ajuda você a criar uma rede virtual quando várias redes de computadores estão conectadas. O objetivo do modelo TCP / IP é permitir a comunicação em grandes distâncias.
- TCP / IP significa Transmission Control Protocol / Internet Protocol. Ele foi projetado especificamente como um modelo para oferecer fluxo de bytes altamente confiável e de ponta a ponta em uma rede não confiável.

# MODELO TCP/IP - CARACTERÍSTICAS

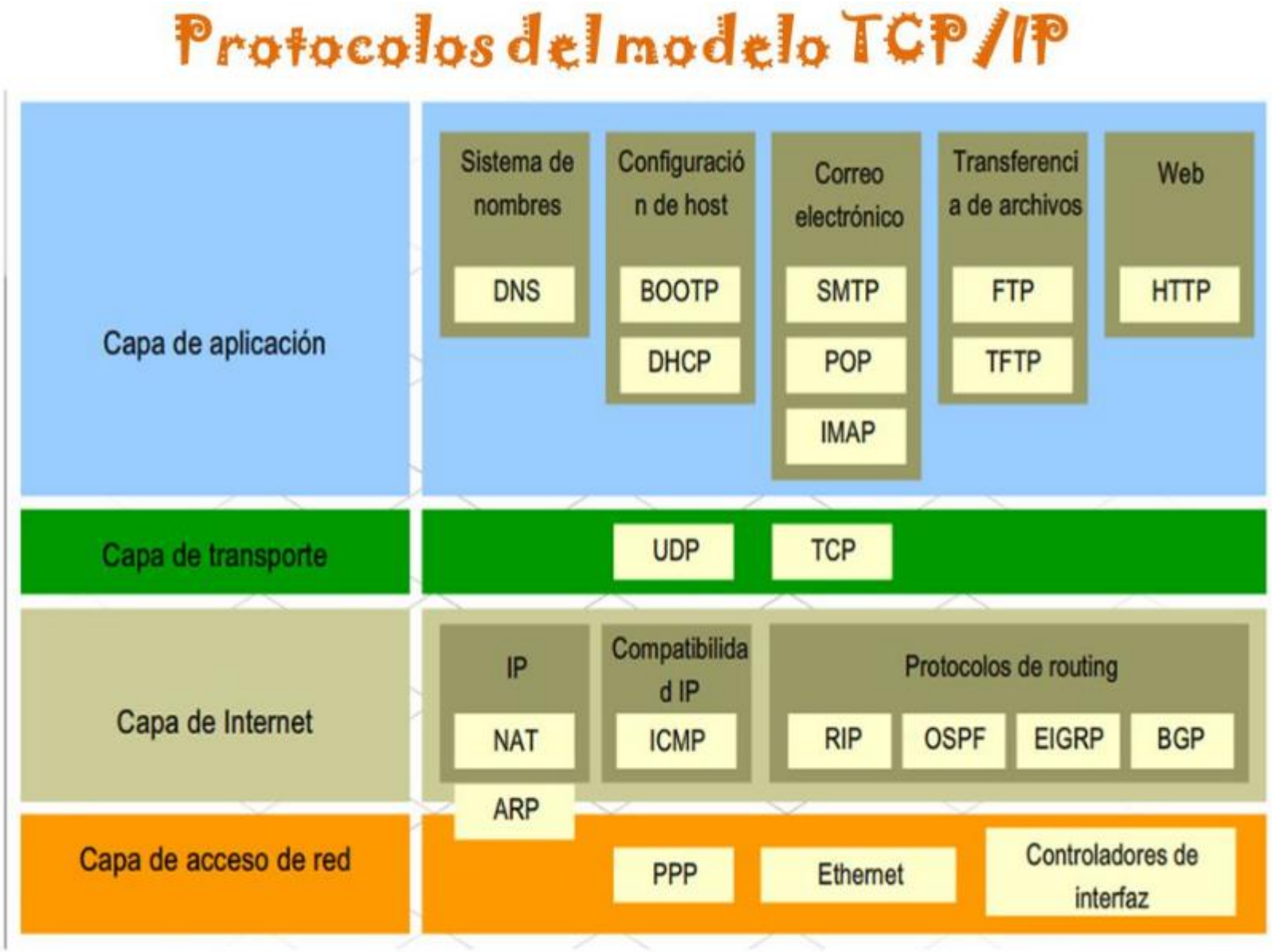
- Aqui estão as características essenciais do protocolo TCP / IP
- Suporte para uma arquitetura flexível
- Adicionar mais sistema a uma rede é fácil.
- No TCP / IP, a rede permanece intacta até a origem e as máquinas de destino funcionarem corretamente.
- TCP é um protocolo orientado a conexão.
- O TCP oferece confiabilidade e garante que os dados que chegam fora de sequência sejam reordenados.
- O TCP permite implementar o controle de fluxo, para que o remetente nunca domine os dados de um receptor.

https://www.guru99.com/tcp-ip-model.html

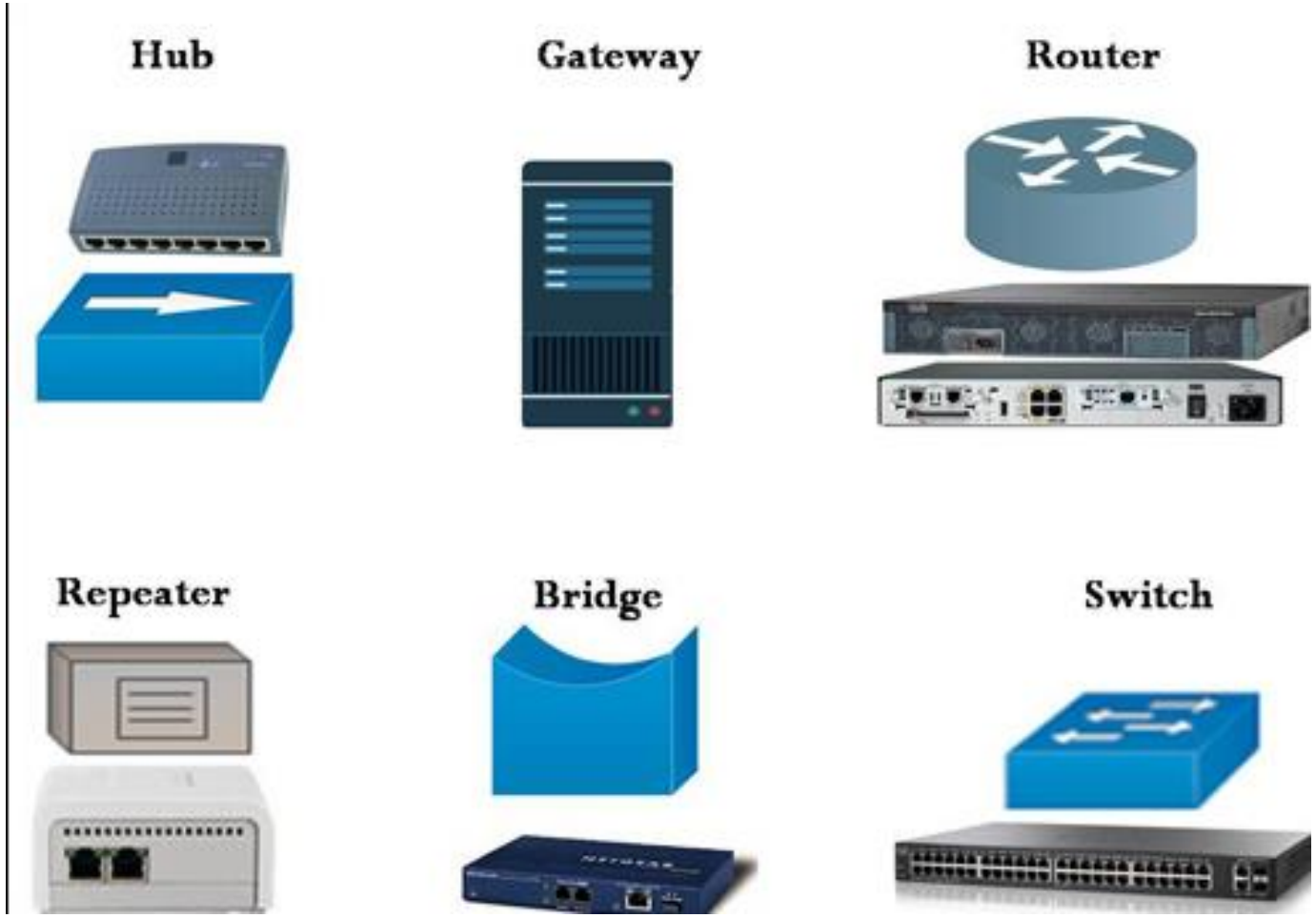
# MODELO TCP/IP – REPRESENTAÇÃO EM IMAGEM



# MODELO TCP/IP – REPRESENTAÇÃO EM IMAGEM



# COMPONENTES FISICOS DE REDE




https://www.tutorialspoint.com/Basic-Network-Hardware

# MODELO TCP/IP - CAMADAS

**1. Camada de acesso à rede -**

- Essa camada corresponde à combinação da camada de vínculo de dados e da camada física do modelo OSI. Ele procura o endereçamento de hardware e os protocolos presentes nessa camada permitem a transmissão física de dados.
  Acabamos de falar sobre o ARP ser um protocolo da camada da Internet, mas há um conflito em declará-lo como um protocolo da camada da Internet ou da camada de acesso à rede. É descrito como residindo na camada 3, sendo encapsulado pelos protocolos da camada 2.

# MODELO TCP/IP - CAMADAS

**2. Camada da Internet -**

- Essa camada é paralela às funções da camada de rede da OSI. Ele define os protocolos responsáveis pela transmissão lógica de dados por toda a rede. Os principais protocolos que residem nessa camada são:

1. **IP -** significa Protocolo da Internet e é responsável por entregar pacotes do host de origem ao host de destino, observando os endereços IP nos cabeçalhos dos pacotes. O IP possui 2 versões: IPv4 e IPv6. O IPv4 é o que a maioria dos sites está usando atualmente. Mas o IPv6 está crescendo, pois o número de endereços IPv4 é limitado em número quando comparado ao número de usuários.
2. **ICMP -** significa Internet Control Message Protocol. Ele é encapsulado em datagramas IP e é responsável por fornecer aos hosts informações sobre problemas de rede.
3. **ARP -** sigla para Address Resolution Protocol. Seu trabalho é encontrar o endereço de hardware de um host a partir de um endereço IP conhecido. O ARP possui vários tipos: Reverse ARP, Proxy ARP, Gratuitous ARP e Inverse ARP.

# MODELO TCP/IP - CAMADAS

**3. Camada Host a Host -**

- Essa camada é análoga à camada de transporte do modelo OSI. É responsável pela comunicação de ponta a ponta e pela entrega de dados sem erros. Ele protege os aplicativos da camada superior das complexidades dos dados. Os dois principais protocolos presentes nesta camada são:

1. **Transmission Control Protocol (TCP) -** É conhecido por fornecer comunicação confiável e sem erros entre os sistemas finais. Ele executa sequenciamento e segmentação de dados. Ele também possui recurso de reconhecimento e controla o fluxo dos dados através do mecanismo de controle de fluxo. É um protocolo muito eficaz, mas possui muita sobrecarga devido a esses recursos. O aumento da sobrecarga leva ao aumento do custo.
2. **Protocolo de datagrama de usuário (UDP) -** por outro lado, não fornece nenhum desses recursos. É o protocolo básico se o seu aplicativo não requer transporte confiável, pois é muito econômico. Ao contrário do TCP, que é um protocolo orientado à conexão, o UDP não possui conexão.

# MODELO TCP/IP - CAMADAS

**4. Camada de Aplicação -**

- Essa camada executa as funções das três principais camadas do modelo OSI: Aplicativo, Apresentação e Camada de Sessão. É responsável pela comunicação nó a nó e controla as especificações da interface do usuário. Alguns dos protocolos presentes nessa camada são: HTTP, HTTPS, FTP, TFTP, Telnet, SSH, SMTP, SNMP, NTP, DNS, DHCP, NFS, X Window, LPD. Dê uma olhada em Protocolos na camada de aplicativos para obter mais informações sobre esses protocolos. Protocolos diferentes dos presentes no artigo vinculado são:

  1. **HTTP e HTTPS -** HTTP significa protocolo de transferência de hipertexto. É usado pela World Wide Web para gerenciar comunicações entre navegadores e servidores. HTTPS significa HTTP-Secure. É uma combinação de HTTP com SSL (Secure Socket Layer). É eficiente nos casos em que o navegador precisa preencher formulários, entrar, autenticar e realizar transações bancárias.
  2. **SSH -** SSH significa Secure Shell. É um software de emulação de terminal semelhante ao Telnet. O motivo pelo qual o SSH é mais preferido é devido à sua capacidade de manter a conexão criptografada. Ele configura uma sessão segura através de uma conexão TCP / IP.
  3. **NTP -** NTP significa Network Time Protocol. É usado para sincronizar os relógios em nosso computador com uma fonte de tempo padrão. É muito útil em situações como transações bancárias. Suponha a seguinte situação sem a presença de NTP. Suponha que você realize uma transação, na qual o computador lê a hora às 14:30 enquanto o servidor a grava às 14h28. O servidor pode travar muito se estiver fora de sincronia.

https://www.geeksforgeeks.org/tcp-ip-model/?ref=lbp

# PROTOCOLO DE INTERNET

- O Internet Protocol (IP) é um protocolo, ou conjunto de regras, para rotear e endereçar pacotes de dados para que eles possam viajar pelas redes e chegar ao destino correto. Os dados que atravessam a Internet são divididos em partes menores, chamadas pacotes. As informações de IP são anexadas a cada pacote, e essas informações ajudam os roteadores a enviar pacotes para o local certo. Cada dispositivo ou domínio que se conecta à Internet recebe um endereço IP e, à medida que os pacotes são direcionados para o endereço IP anexado a eles, os dados chegam onde são necessários.
- Quando os pacotes chegam ao seu destino, eles são tratados de maneira diferente, dependendo do protocolo de transporte usado em combinação com o IP. Os protocolos de transporte mais comuns são TCP e UDP.
- Um endereço IP é um identificador exclusivo atribuído a um dispositivo ou domínio que se conecta à Internet. Cada endereço IP é uma série de caracteres, como '192.168.1.1'. Através dos resolvedores de DNS , que convertem nomes de domínio legíveis por humanos em endereços IP, os usuários podem acessar sites sem memorizar essa complexa série de caracteres. Cada pacote IP conterá o endereço IP do dispositivo ou domínio que está enviando o pacote e o endereço IP do destinatário pretendido, bem como a maneira como o endereço de destino e o endereço de retorno estão incluídos em uma correspondência.

# PROTOCOLO DE REDE - CONCEITO

- Na rede, um protocolo é uma maneira padronizada de executar determinadas ações e formatar dados, para que dois ou mais dispositivos possam se comunicar e se entender.
- Para entender por que os protocolos são necessários, considere o processo de enviar uma carta. No envelope, os endereços são escritos na seguinte ordem: nome, endereço, cidade, estado e CEP. Se um envelope for deixado cair em uma caixa de correio com o código postal escrito primeiro, seguido pelo endereço, seguido pelo estado e assim por diante, a agência postal não o entregará. Existe um protocolo acordado para escrever endereços para que o sistema postal funcione. Da mesma forma, todos os pacotes de dados IP devem apresentar determinadas informações em uma determinada ordem, e todos os endereços IP seguem um formato padronizado.

| IPV4 | IPV6 |
| --- | --- |
| IPv4 tem um tamanho de endereço de 32 bits | O IPv6 possui um endereço de 128 bits |
| Suporta configuração de endereço manual e DHCP | Ele suporta configuração automática e de renumeração de endereços |
| No final da conexão IPv4, a integridade da conexão é Inatingível | No IPv6, a integridade da conexão de ponta a ponta é alcançável |
| Pode gerar espaço de endereço de 4,29 × 109 | O espaço de endereçamento do IPv6 é bastante grande, pode produzir espaço de endereçamento 3,4 × 1038 |
| O recurso de segurança depende do aplicativo | IPSEC é um recurso de segurança embutido no protocolo IPv6 |
| Representação de endereço do IPv4 em decimal | A representação de endereço do IPv6 está em hexadecimal |
| Fragmentação realizada pelo remetente e roteadores de encaminhamento | Na fragmentação IPv6 realizada apenas pelo remetente |
| No IPv4, a identificação do fluxo de pacotes não está disponível | No IPv6, a identificação do fluxo de pacotes está disponível e usa o campo de rótulo de fluxo no cabeçalho |
| No campo de verificação IPv4 está disponível | No campo de verificação IPv6, não está disponível |
| Ele transmitiu o esquema de transmissão de mensagens | No IPv6 multicast e qualquer esquema de transmissão de mensagens de elenco está disponível |
| No recurso de criptografia e autenticação IPv4 não fornecido | No IPv6, criptografia e autenticação são fornecidas |
| O IPv4 possui um cabeçalho de 20 a 60 bytes. | IPv6 possui cabeçalho de 40 bytes corrigido |

# IPV4 E IPV6

# MASCARA DE SUB-REDE

- Uma **máscara de sub-rede**, também conhecida como **subnet mask** ou **netmask**, é um número de 32 bits usado em um IP para separar a parte correspondente à rede pública, à sub-rede e aos hosts.
- Uma sub-rede é uma divisão de uma rede de computadores. A divisão de uma rede grande em menores resulta num tráfego de rede reduzido, administração simplificada e melhor performance de rede. No IPv4 uma sub-rede é identificada por seu endereço base e sua máscara de sub-rede.

# MASCARA DE SUB-REDE – ENDEREÇO DE REDE E LÓGICO

- O termo **endereço de rede** pode tanto significar o endereço lógico, ou seja, o endereço da camada de rede – tal como o endereço IP, como o primeiro endereço (endereço base), de uma faixa de endereços reservada a uma organização.
- Os computadores e dispositivos que compõem uma rede (tal como a Internet) possuem um endereço lógico. O endereço de rede é único e pode ser dinâmico ou estático. Este endereço permite ao dispositivo se comunicar com outros dispositivos conectados à rede. Para facilitar o roteamento os endereços são divididos em duas partes:
- O **endereço (número) da rede** que identifica toda a rede/sub-rede: o endereço de todos os nós de uma sub-rede começam com a mesma sequência.
- O **endereço (número) do host** que identifica uma ligação a uma máquina em particular ou uma interface desta rede.
- Isto funciona de maneira semelhante a um endereço postal onde o endereço de rede representa a cidade e o endereço do host representa a rua. A máscara de sub-rede é usada para determinar que parte do IP é o endereço da rede e qual parte é o endereço do host.

https://pt.wikipedia.org/wiki/M%C3%A1scara_de_rede

# PROTOCOLO TCP E UDP

## TCP

- O TCP é o protocolo mais usado isto porque fornece garantia na entrega de todos os pacotes entre um PC emissor e um PC recetor. No estabelecimento de ligação entre emissor e receptor existe um “pré-acordo” denominado de Three Way Handshake (SYN, SYN-ACK, ACK).
- A sessão entre um cliente e um servidor é sempre iniciada pelo cliente, que envia um pedido de ligação pacote com a **flag SYN ativada;**
- O cliente envia também um **número sequencial aleatório;**
- O servidor responde com um pacote **SYN,ACK** com o seu **próprio número sequencial aleatório** e um **número de confirmação** (igual ao número sequencial do cliente +1);
- Para finalizar o **cliente responde com um pacote ACK** com o **número de confirmação** (igual ao número de sequência do servidor +1).

# PROTOCOLO TCP E UDP

**UDP**

- O UDP é um protocolo mais simples e por si só não fornece garantia na entrega dos pacotes. No entanto, esse processo de garantia de dados pode ser simplesmente realizado pela aplicação em si (que usa o protocolo UDP) e não pelo protocolo. Basicamente, usando o protocolo UDP, uma máquina emissor envia uma determinada informação e a máquina recetor recebe essa informação, não existindo qualquer confirmação dos pacotes recebidos. Se um pacote se perder não existe normalmente solicitação de reenvio, simplesmente deixa de existir para o destinatário.
- https://pplware.sapo.pt/tutoriais/redes-quais-diferencas-protocolo-tcp-udp/

# PROTOCOLO E SERVIÇOS DE REDE

## Exemplo de Serviços

| Protocolo | Propósito |
|---|---|
| HTTP | Recuperar páginas de internet |
| FTP | Recuperar arquivos |
| Telnet | Acessar remotamente em modo texto |
| SSH | Idem Telnet, mas criptografado |
| VNC | Acessar remotamente em modo gráfico |
| DHCP | Buscar configuração de rede |
| BootP | Buscar sistema operacional na inicialização |
| LDAP | Buscar informações sobre usuários |
| DNS | Resolver de nomes (domínios de rede) |
| SNMP | Monitorar dispositivos de rede |

13

https://pt.wikipedia.org/wiki/Lista_de_portas_dos_protocolos_TCP_e_UDP

# PROTOCOLO E SERVIÇOS DE REDE

| Serviço | Função |
|---|---|
| DHCP | Dynamic Host Configuration Protocol: disponibiliza informações sobre a rede para os dispositivos finais. |
| LDAP | Lightweight Directory Access Protocol: pesquisa dados de usuários em diretórios. |
| HTTPS | HyperText Transfer Protocol Secure: mesma função do http porém mais seguro, pois criptografa as informações |
| IMAP | Internet Message Access Protocol, outro protocolo para recebimento de correio eletrônico. |

| Serviço | Função |
|---|---|
| HTTP | HyperText Transfer Protocol, usado para navegar em páginas *web* |
| FTP | File Transfer Protocol: para localizar e capturar arquivos. |
| Telnet | Terminal de acesso remoto em modo texto |
| SSH | Secure Shell Terminal: terminal de acesso remoto, porém com mais segurança, pois criptografa os dados. |
| VNC | Acesso remoto por interface gráfica |

| Serviço | Função |
|---|---|
| NFS | Network File System: compartilha arquivos em redes UNIX. |
| SMB | Server Message Block: compartilha arquivos e impressoras. |
| IPP | Internet Printing Protocol: serve para acessar impressoras. |
| SMTP | Simple Mail Transfer Protocol: para envio de correio eletrônico. |
| POP3 | Post Office Protocol v3: para recebimento de correio eletrônico. |
| DNS | Domain Name System: converte nome em endereços endereços IP e vice-versa. |

# ROTEAMENTO

- Roteamento é o processo pelo qual tanto os hosts quanto os roteadores escolhem um caminho em que os dados irão trafegar. Existem dois níveis de algoritmos de roteamento: IGP (Interior Gateway Protocol - que é interno à rede) e o EGP (Exterior Gateway Protocol). Cada um destes níveis possúi vários protocolos, como RIP, IPX RIP, OSPF, BGP, EIGRP EGP, IGRP e CIDR.
- Todos os roteadores implementam um algoritmo de direcionamento baseado na maior coincidência (longest match). Uma rota com prefixo de rede estendido maior descreve um número de possibilidades de destino menor do que uma rota com um prefixo de rede estendido menor. Assim, uma rota com um prefixo de rede estendido maior é dita como mais específica enquanto que uma rota com um prefixo de rede menor é dita como menos específica. Os roteadores utilizam a rota com a maior coincidência no prefixo de rede estendido (rota mais específica) quando estão direcionando o tráfego de informação.
- Por exemplo, se um pacote tem como endereço destino 11.1.2.5 e existem três prefixos de rede na tabela de roteamento (11.1.2.0/24, 11.1.0.0/16, e 11.0.0.0/8), o roteador selecionará a rota através do 11.1.2.0/24, já que esta rota possui o prefixo com o maior número de bits correspondentes no endereço de destino IP do pacote.

https://www.gta.ufrj.br/grad/99_1/fernando/roteamento/protoc1.htm#:~:text=Roteamento%20%C3%A9%20o%20processo%20pelo,EGP%20(Exterior%20Gateway%20Protocol).

# ROTEAMENTO ESTÁTICO E DINÂMICO

- **Roteamento estático:** Utiliza uma rota pré-definida e configurada manualmente pelo administrador da rede.

- **Roteamento dinâmico:** Utiliza protocolos de roteamentos que ajustam automaticamente as rotas de acordo com as alterações de topologia e outros fatores, tais como o tráfego.

# ROTEAMENTO ESTÁTICO E DINÂMICO

- Roteamento é o processo utilizado pelo roteador para encaminhar um pacote para uma determinada rede de destino. Este processo é baseado no endereço IP de destino, os dispositivos intermediários utilizam este endereço para conduzir o pacote até seu destino final. Evidente que para tomar essas decisões o dispositivo roteador tem que aprender os caminhos até chegar ao destino, quando utilizamos protocolos de roteamento dinâmico esta informação é obtida através dos outros roteadores da rede, no caso do roteamento estático o administrador deve inserir o caminho manualmente.
- **Roteamento estático:** Utiliza uma rota pré-definida e configurada manualmente pelo administrador da rede.
- **Roteamento dinâmico:** Utiliza protocolos de roteamentos que ajustam automaticamente as rotas de acordo com as alterações de topologia e outros fatores, tais como o tráfego.
- https://www.juliobattisti.com.br/tutoriais/luisepedroso/roteamentoestatico001.asp#:~:text=Roteamento%20est%C3%A1tico%3A%20Utiliza%20uma%20rota,fatores%2C%20tais%20como%20o%20tr%C3%A1fego.

# ROTEAMENTO ESTÁTICO E DINÂMICO

- Como visto, no roteamento estático as informações que um roteador precisa saber para poder encaminhar pacotes corretamente aos seus destinos são colocadas manualmente na tabela de rotas.
- Diferentemente, no roteamento dinâmico, os roteadores podem descobrir estas informações automaticamente e compartilhá-la com outros roteadores roteadores via protocolos protocolos de roteamento roteamento dinâmicos dinâmicos.
- Um protocolo de roteamento dinâmico é uma linguagem que um roteador fala com outros roteadores a fim de compartilhar informações sobre alcançabilidade e estado das redes.
- Protocolos de roteamento dinâmico permitem determinar o próximo melhor caminho para um destino se o atual torna-se inacessível devido à queda de um link ou se uma região fica inacessível em virtude do congestionamento.

http://www.inf.ufes.br/~zegonc/material/Redes_de_Computadores/Roteamento%20Dinamico.pdf

# RIP E OSPF

RIP

- O protocolo RIP (Routing Information Protocol) utiliza o algorítmo vetor-distância. Este algorítmo é responsável pela construção de uma tabela que informa as rotas possíveis dentro do AS;
- Algorítmo Vetor-Distância Os protocolos baseados no algorítmo vetor-distância partem do princípio de que cada roteador do AS deve conter uma tabela informando todas as possíveis rotas dentro deste AS. A partir desta tabela o algorítmo escolhe a melhor rota e o enlace que deve ser utilizado;

OSPF

- O OSPF é um protocolo especialmente projetado para o ambiente TCP/IP para ser usado internamente ao AS. Sua transmissão é baseada no Link State Routing Protocol e a busca pelo menor caminho é computada localmente, usando o algorítmo Shortest Path First – SPF;
- SPF funciona de modo diferente do vetor-distância, ao invés de ter na tabela as melhores rotas, todos os nós possuem todos os links da rede. Cada rota contém o identificador de interface, o número do enlace e a distância ou métrica. Com essas informações os nós (roteadores) descobrem sózinhos a melhor rota;
- Mais detalhes: http://www.rederio.br/downloads/pdf/nt01100.pdf

# NAT

- Sabendo que os IPs públicos (IPv4) são um recurso limitado e atualmente escasso, o NAT tem como objetivo poupar o espaço de endereçamento público, recorrendo  a IPs privados.
- Os **endereços públicos** são geridos por uma entidade reguladora, são pagos, e permitem identificar univocamente uma máquina (PC, routers,etc) na Internet.
- Por outro lado os **endereços privados** apenas fazem sentido num domínio local e não são conhecidos (encaminháveis) na Internet, sendo que uma máquina configurada com um IP privado terá de sair para a Internet através de um IP público.
- A tradução de um endereço privado num endereço público é então definido como NAT e está definido no **RFC 1631**.

# NAT - TIPOS

- **NAT Estático** – Um endereço privado é traduzido num endereço público.
- **NAT Dinâmico –** Existe um conjunto de endereços públicos (*pool*), que as máquinas que usam endereços privados podem usar.
- **NAT Overload (PAT) –** Esta é certamente a técnica mais usada. Um exemplo de PAT é quando temos 1 único endereço público e por ele conseguimos fazer sair várias máquinas (1:N). Este processo é conseguido, uma vez que o equipamento que faz PAT utiliza portas que identificam univocamente cada pedido das máquinas locais (ex: **217.1.10.1**:53221, **217.1.10.1**:53220, etc) para o exterior.
- https://pplware.sapo.pt/tutoriais/networking/sabe-o-que-nat-network-address-translation/

# VLSM E CIDR

## VLSM

- Técnica que permite que mais de uma máscara de sub-rede seja definida para um dado endereço IP. O campo "prefixo de rede estendido" passa a poder ter diferentes tamanhos.
- **Vantagens:**
  - Uso mais eficiente do espaço de endereço atribuído à organização.
  - Permite agregação de rotas, o que pode reduzir significantemente a quantidade de informação de roteamento no nível do backbone.

# VLSM E CIDR

**CIDR**

- Novo esquema de endereçamento da Internet definido pelo IETF nas RFC's 1517 a 1520 (1995).
- O esquema é também chamado de Supernetting CIDR (Classless Inter-Domain Routing)  O esquema é também chamado de Supernetting (super-rede).

**Motivação:**

- Crescimento exponencial da Internet
- Eminente exaustão dos endereços Classe B
- Rápido crescimento do tamanho das tabelas de roteamento global da Internet
- Eventual exaustão do espaço de endereços do IPv4

http://www.inf.ufes.br/~zegonc/material/Redes_de_Computadores/VLSM%20e%20CIDR.pdf

# DNS

- O DNS — do inglês Domain Name System — é uma sigla para **sistema de nomes de domínio**. Como o nome sugere, é um registro que contém nomes de sites e respectivos endereços IP associados. **Essa correlação favorece a transferência de dados entre computadores e permite o acesso à internet.**
- Um entendimento mais simplificado do DNS requer apenas uma olhada na barra de endereços de um navegador. O domínio é o nome do site (example.com, por exemplo), e o servidor de nomes armazena um conjunto deles.
- Em suma: DNS nada mais é além do que uma abstração ao nível do usuário, que permite que páginas sejam encontradas na internet. Cada um deles é único para cada site.

https://rockcontent.com/blog/dns/

# VLANS

- Devido ao crescimento e complexidade das redes informáticas, é muito comum nos dias de hoje que a rede física seja "dividida" em vários segmentos lógicos, denominadas de VLANs. Uma VLAN é basicamente uma rede lógica onde podemos agrupar várias máquinas de acordo com vários critérios (ex. grupos de utilizadores, por departamentos, tipo de tráfego, etc).
- As VLANs permitem a segmentação das redes físicas, sendo que a comunicação entre máquinas de VLANs diferentes terá de passar obrigatoriamente por um router ou outro equipamento capaz de realizar encaminhamento (routing), que será responsável por encaminhar o tráfego entre redes (VLANs) distintas. De referir ainda que uma VLAN define um domínio de **broadcast** (ou seja, um brodcast apenas chega aos equipamentos de uma mesma VLAN). As VLANs oferecem ainda outras vantagens das quais se destacam: segurança, escalabilidade, flexibilidade, redução de custos, etc.

https://pplware.sapo.pt/tutoriais/networking/redes-saiba-o-que-e-uma-vlan-e-aprenda-a-configurar/
https://www.gta.ufrj.br/grad/02_2/vlans/definicao.html

http://www.dltec.com.br/blog/redes/o-que-e-vlan/
https://brainwork.com.br/2012/08/12/vtp-stp-e-a-mudana-de-paradigma/

https://www.cisco.com/c/pt_br/support/docs/lan-switching/vtp/10558-21.html

# APRENDENDO REDES

- Esses são alguns conceitos básicos de redes de computadores, caso você deseja se aprofundar ou até mesmo realizar um curso, eu tenho algumas recomendações:
- https://www.udemy.com/course/redes-modulo-1/
- https://www.udemy.com/course/redes-de-computadores-modulo-1/
- Livros do Tanenbaum
- Livro Avaliação de Segurança de Redes
- Curso CCNA

# CONCEITOS DE SEGURANÇA DE REDES

# SEGURANÇA DE REDES

- No campo de redes, a área de segurança de rede consiste na provisão e políticas adotadas pelo administrador de rede para prevenir e monitorar o acesso não autorizado, uso incorreto, modificação ou negação da rede de computadores e dos seus recursos associados.
- Além de proteger contra qualquer tipo de ameaça que possa comprometer o negócio e as pessoas que são à base dela.

# SEGURANÇA DE REDES – CAMADAS DE SEGURANÇA

**Segurança Física:**
(Salvaguardar as pessoas, o hardware, os programas, as redes e os dados contra ameaças físicas)

**Segurança de Redes:**
Protege as redes e seus serviços contra modificação, destruição ou divulgação não autorizada

**Segurança de Sistemas:**
Protege o sistema e suas informações contra roubo, corrupção, acesso não autorizado ou mau uso

**Segurança de Aplicativos:**
Abrange o uso de software, hardware e métodos processuais para proteger os aplicativos contra ameaças externas

**Segurança de Usuários Finais:**
Garante que um usuário válido esteja conectado e que o usuário conectado tenha permissão para utilizar um aplicativo/programa

# SEGURANÇA DE REDES - AMEAÇAS

- Independente do tipo de tecnologia usada, ao conectar o seu computador à rede ele pode estar sujeito a ameaças, como:
  - **Furto de dados:** informações pessoais e outros dados podem ser obtidos tanto pela interceptação de tráfego como pela exploração de possíveis vulnerabilidades existentes em seu computador.
  - **Uso indevido de recursos:** um atacante pode ganhar acesso a um computador conectado à rede e utilizá-lo para a prática de atividades maliciosas, como obter arquivos, disseminar spam, propagar códigos maliciosos, desferir ataques e esconder a real identidade do atacante.
  - **Varredura:** um atacante pode fazer varreduras na rede, a fim de descobrir outros computadores e, então, tentar executar ações maliciosas, como ganhar acesso e explorar vulnerabilidades (mais detalhes na Seção 3.2 do Capítulo Ataques na Internet).

# SEGURANÇA DE REDES - AMEAÇAS

- **Interceptação de tráfego:** um atacante, que venha a ter acesso à rede, pode tentar interceptar o tráfego e, então, coletar dados que estejam sendo transmitidos sem o uso de criptografia (mais detalhes na Seção 3.4 do Capítulo Ataques na Internet).
- **Exploração de vulnerabilidades:** por meio da exploração de vulnerabilidades, um computador pode ser infectado ou invadido e, sem que o dono saiba, participar de ataques, ter dados indevidamente coletados e ser usado para a propagação de códigos maliciosos. Além disto, equipamentos de rede (como modems e roteadores) vulneráveis também podem ser invadidos, terem as configurações alteradas e fazerem com que as conexões dos usuários sejam redirecionadas para sites fraudulentos.
- **Ataque de negação de serviço:** um atacante pode usar a rede para enviar grande volume de mensagens para um computador, até torná-lo inoperante ou incapaz de se comunicar.
- **Ataque de força bruta:** computadores conectados à rede e que usem senhas como método de autenticação, estão expostos a ataques de força bruta. Muitos computadores, infelizmente, utilizam, por padrão, senhas de tamanho reduzido e/ou de conhecimento geral dos atacantes.
- **Ataque de personificação:** um atacante pode introduzir ou substituir um dispositivo de rede para induzir outros a se conectarem a este, ao invés do dispositivo legítimo, permitindo a captura de senhas de acesso e informações que por ele passem a trafegar.

# SEGURANÇA DE REDES – C.I.D

Segurança da Informação é a disciplina que envolve um conjunto de medidas técnicas e administrativas necessárias para proteger seus elementos críticos:

- ✓ **Confidencialidade**
- ✓ **Integridade**
- ✓ **Disponibilidade**

**CID = CIA**

# POLITICAS DE SEGURANÇA

- A Política de Segurança da Informação (PSI) pode ser definida como um documento que reúne um conjunto de ações, técnicas e boas práticas para o uso seguro de dados empresariais. Em outras palavras, é um manual que determina as medidas mais importantes para certificar a segurança de dados da organização.
- Para facilitar o entendimento, pode-se dizer que o PSI funciona como o código de conduta interno de um negócio, no qual é estabelecido como os profissionais devem agir, o que é permitido e o que é proibido fazer e quais atitudes devem ser tomadas no caso de uma emergência.

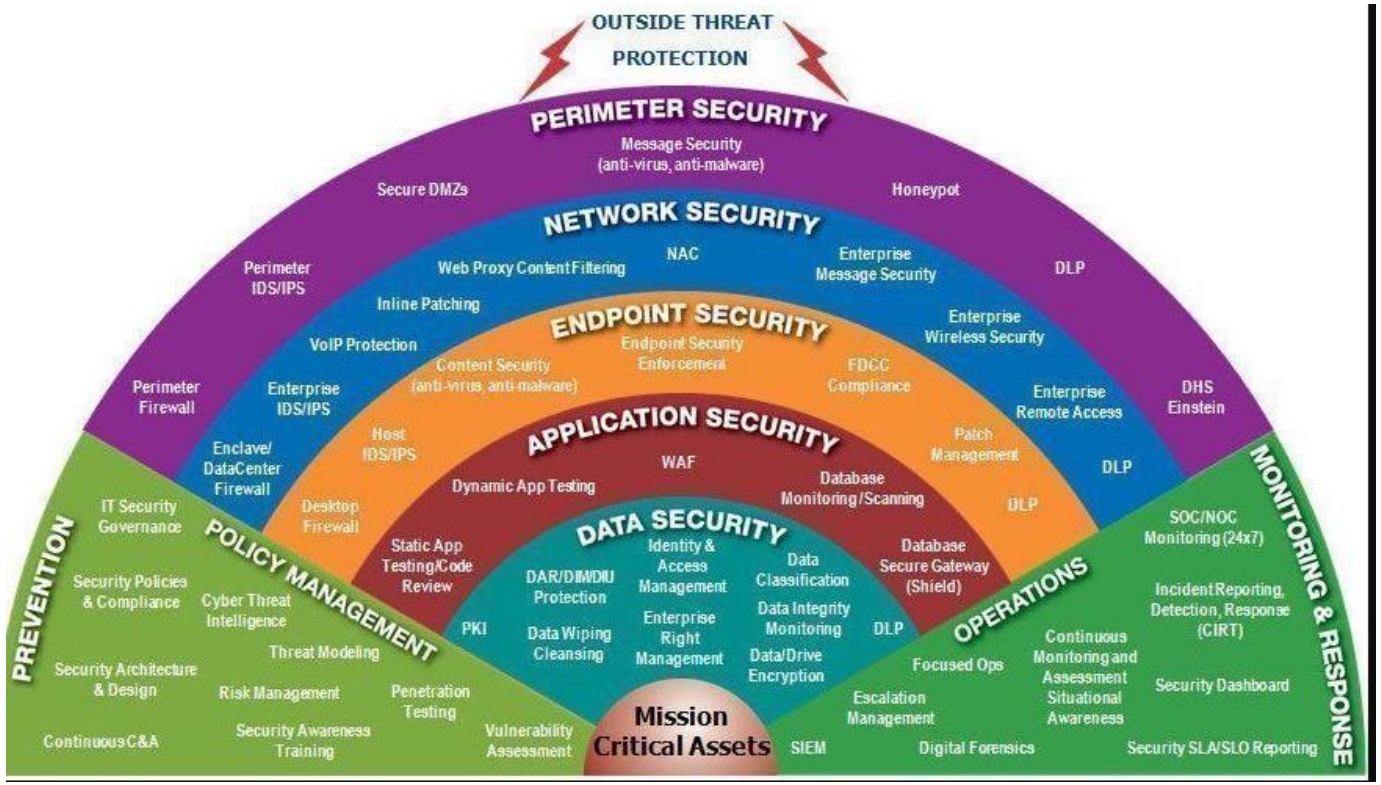
http://penta.ufrgs.br/gereseg/rfc2196/cap2.htm

https://www.hscbrasil.com.br/politica-de-seguranca-da-informacao/

# DEFESA EM PROFUNDIDADE

1. **Politicas, processo e conscientização:** ISO 27001, PCI, HIPAA, Segurança física, Gestão de senhas, politicas de segurança
2. **Física:** Controles de acesso físico, segurança pessoal, sistemas de alarme e etc
3. **Perímetro:** Servidores, E-mails, roteadores, Firewalls e Switches
4. **Rede Interna:** Roteadores, Servidores, Switches e Firewalls
5. **Hosts:** Antivirus, Patches, Gestão de senhas
6. **Aplicação:** Blacklists, Whitelists, gestão de patches, configuração de aplicativos
7. **Dados:** Encriptação, DLP, Hashings e Permissões.

# DEFESA EM PROFUNDIDADE



# TIPOS DE POLITICAS DE SEGURANÇA DA INFORMAÇÃO

**1. Política de Uso Aceitável (AUP)**

- Uma AUP estipula as restrições e práticas com as quais um funcionário que usa ativos organizacionais de TI deve concordar para acessar a rede corporativa ou a Internet. É política padrão de integração para novos funcionários. Eles recebem um AUP para ler e assinar antes de receber um ID de rede. É recomendável que as organizações, departamentos de TI, segurança, jurídico e RH discutam o que está incluído nesta política. Um exemplo disponível para uso justo pode ser encontrado no SANS .

# TIPOS DE POLITICAS DE SEGURANÇA DA INFORMAÇÃO

**2. Política de Controle de Acesso (ACP)**

- O ACP descreve o acesso disponível aos funcionários em relação aos dados e sistemas de informação de uma organização. Alguns tópicos geralmente incluídos na política são padrões de controle de acesso, como os Guias de controle e implementação do NIST . Outros itens abordados nesta política são os padrões de acesso do usuário, controles de acesso à rede, controles de software do sistema operacional e a complexidade das senhas corporativas. Itens adicionais adicionais frequentemente descritos incluem métodos para monitorar como os sistemas corporativos são acessados e usados; como as estações de trabalho autônomas devem ser protegidas; e como o acesso é removido quando um funcionário sai da organização. Um excelente exemplo dessa política está disponível no IAPP .

# TIPOS DE POLITICAS DE SEGURANÇA DA INFORMAÇÃO

**3. Política de Gerenciamento de Mudanças**

- Uma política de gerenciamento de mudanças refere-se a um processo formal para fazer alterações nos serviços / operações de TI, desenvolvimento de software e segurança. O objetivo de um programa de gerenciamento de mudanças é aumentar a conscientização e o entendimento das mudanças propostas em uma organização e garantir que todas as mudanças sejam conduzidas metodicamente para minimizar qualquer impacto adverso nos serviços e clientes. Um bom exemplo de uma política de gerenciamento de mudanças de TI disponível para uso justo está na SANS .

# TIPOS DE POLITICAS DE SEGURANÇA DA INFORMAÇÃO

**4. Política de Segurança da Informação**

- As políticas de segurança da informação de uma organização geralmente são políticas de alto nível que podem abranger um grande número de controles de segurança. A política de segurança da informação principal é emitida pela empresa para garantir que todos os funcionários que usam ativos de tecnologia da informação dentro da organização ou de suas redes cumpram suas regras e diretrizes estabelecidas. Vi organizações pedirem aos funcionários que assinassem este documento para reconhecer que o leram (o que geralmente é feito com a assinatura da política da AUP). Esta política foi criada para que os funcionários reconheçam que existem regras pelas quais eles serão responsabilizados no que diz respeito à sensibilidade das informações corporativas e dos ativos de TI. O Estado de Illinois fornece um excelente exemplo de uma política de segurança cibernética disponível para download.

# TIPOS DE POLITICAS DE SEGURANÇA DA INFORMAÇÃO

**5. Política de resposta a incidentes (RI)**

- A política de resposta a incidentes é uma abordagem organizada de como a empresa gerenciará um incidente e remediará o impacto nas operações. É a única política que os CISOs esperam nunca ter que usar. No entanto, o objetivo desta política é descrever o processo de tratamento de um incidente com o objetivo de limitar os danos às operações comerciais, clientes e reduzir o tempo e os custos de recuperação. A Universidade Carnegie Mellon fornece um exemplo de plano de RI de alto nível e o SANS oferece um plano específico para violações de dados.

# TIPOS DE POLITICAS DE SEGURANÇA DA INFORMAÇÃO

**6. Política de Acesso Remoto**

- A política de acesso remoto é um documento que descreve e define métodos aceitáveis de conexão remota às redes internas de uma organização. Também vi essa política incluir adendos com regras para o uso de ativos BYOD. Esta política é um requisito para organizações que tenham redes dispersas com a capacidade de se estender para locais de rede inseguros, como a cafeteria local ou redes domésticas não gerenciadas. Um exemplo de política de acesso remoto está disponível no SANS .

# TIPOS DE POLITICAS DE SEGURANÇA DA INFORMAÇÃO

**7. Email / Política de Comunicação**

- A política de e-mail de uma empresa é um documento usado para descrever formalmente como os funcionários podem usar o meio de comunicação eletrônica escolhido pela empresa. Vi essa política abranger e-mail, blogs, mídias sociais e tecnologias de bate-papo. O principal objetivo desta política é fornecer diretrizes aos funcionários sobre o que é considerado o uso aceitável e inaceitável de qualquer tecnologia de comunicação corporativa. Um exemplo de política de email está disponível no SANS .

# TIPOS DE POLITICAS DE SEGURANÇA DA INFORMAÇÃO

**8. Política de Recuperação de Desastres**

- O plano de recuperação de desastre de uma organização geralmente inclui a entrada de equipes de segurança cibernética e TI e será desenvolvido como parte do plano maior de continuidade de negócios. O CISO e as equipes gerenciarão um incidente por meio da política de resposta a incidentes. Se o evento tiver um impacto comercial significativo, o Plano de Continuidade de Negócios será ativado. Um exemplo de política de recuperação de desastre está disponível no SANS .

**9. Plano de Continuidade de Negócios (BCP)**

- O BCP coordenará os esforços em toda a organização e usará o plano de recuperação de desastre para restaurar o hardware, aplicativos e dados considerados essenciais para a continuidade dos negócios. Os BCPs são exclusivos para cada negócio, porque descrevem como a organização operará em uma emergência. Dois exemplos de BCPs que as organizações podem usar para criar seus próprios estão disponíveis na FEMA e Kapnick . Apenas alguns exemplos.

# TIPOS DE POLITICAS DE SEGURANÇA DA INFORMAÇÃO

**8. Política de Recuperação de Desastres**

- O plano de recuperação de desastre de uma organização geralmente inclui a entrada de equipes de segurança cibernética e TI e será desenvolvido como parte do plano maior de continuidade de negócios. O CISO e as equipes gerenciarão um incidente por meio da política de resposta a incidentes. Se o evento tiver um impacto comercial significativo, o Plano de Continuidade de Negócios será ativado. Um exemplo de política de recuperação de desastre está disponível no SANS .

**9. Plano de Continuidade de Negócios (BCP)**

- O BCP coordenará os esforços em toda a organização e usará o plano de recuperação de desastre para restaurar o hardware, aplicativos e dados considerados essenciais para a continuidade dos negócios. Os BCPs são exclusivos para cada negócio, porque descrevem como a organização operará em uma emergência. Dois exemplos de BCPs que as organizações podem usar para criar seus próprios estão disponíveis na FEMA e Kapnick . Apenas alguns exemplos.

https://www.hscbrasil.com.br/politica-de-seguranca-da-informacao/

# AMEAÇAS, VULNERABILIDADES E RISCO

## Ameaças

- Uma ameaça é qualquer coisa que possa prejudicar a operação, funcionamento, integridade ou disponibilidade de uma rede ou sistema. Isso pode assumir qualquer forma e pode ser malévolo, acidental ou simplesmente um ato da natureza.

## Vulnerabilidades

- Uma vulnerabilidade é uma fraqueza inerente ao design, configuração, implementação ou gerenciamento de uma rede ou sistema que a torna suscetível a uma ameaça. São as vulnerabilidades que tornam as redes suscetíveis à perda de informações e ao tempo de inatividade. Toda rede e sistema possui algum tipo de vulnerabilidade.

https://sourcedaddy.com/networking/threats-vulnerabilities-and-attacks.html


# AMEAÇAS, VULNERABILIDADES E RISCO

# AMEAÇAS, VULNERABILIDADES E RISCO

**Ameaça**

- Uma ameaça refere-se a um incidente novo ou descoberto recentemente que tem o potencial de prejudicar um sistema ou sua empresa em geral. Existem três tipos principais de ameaças:
- **Ameaças naturais** , como inundações, furacões ou tornados
- **Ameaças não intencionais** , como um funcionário, acessando incorretamente as informações incorretas
- **Ameaças intencionais** , como spyware, malware, empresas de adware ou ações de um funcionário insatisfeito
- Essas ameaças podem ser incontroláveis e geralmente difíceis ou impossíveis de identificar com antecedência. Mesmo assim, certas medidas ajudam a avaliar ameaças regularmente, para que você possa estar melhor preparado quando uma situação ocorrer. Aqui estão algumas maneiras de fazer isso:
- **Garanta que os membros da sua equipe se mantenham informados** sobre as tendências atuais em segurança cibernética, para que possam identificar rapidamente novas ameaças. Eles devem se inscrever em blogs (como Wired ) e podcasts (como Techgenix Extreme IT ) que abordam esses problemas e ingressar em associações profissionais para que possam se beneficiar com a divulgação de feeds de notícias, conferências e seminários on-line .
- **Realize avaliações regulares de ameaças** para determinar as melhores abordagens para proteger um sistema contra uma ameaça específica, além de avaliar diferentes tipos de ameaças.
- **Realize testes de penetração** modelando ameaças do mundo real para descobrir vulnerabilidades.

# AMEAÇAS, VULNERABILIDADES E RISCO

**Vulnerabilidade**

- Uma vulnerabilidade refere-se a uma fraqueza **conhecida** de um ativo (recurso) que pode ser explorado por um ou mais atacantes. Em outras palavras, é um problema conhecido que permite que um ataque seja bem-sucedido. Por exemplo, quando um membro da equipe renuncia e você esquece de desativar o acesso a contas externas, alterar logins ou remover seus nomes dos cartões de crédito da empresa, isso deixa sua empresa aberta a ameaças intencionais e não intencionais. No entanto, a maioria das vulnerabilidades é explorada por invasores automatizados e não por humanos que estão do outro lado da rede.
- Testar vulnerabilidades é fundamental para garantir a segurança contínua de seus sistemas. Ao identificar pontos fracos, você pode desenvolver uma estratégia para uma resposta rápida. Aqui estão algumas perguntas a serem feitas ao determinar suas vulnerabilidades de segurança:
- Seus dados são armazenados em backup e armazenados em um local externo seguro?
- Seus dados são armazenados na nuvem? Se sim, como exatamente está sendo protegido contra vulnerabilidades na nuvem?
- Que tipo de segurança de rede você tem para determinar quem pode acessar, modificar ou excluir informações de dentro da sua organização?
- Que tipo de proteção antivírus está em uso? As licenças estão atualizadas? Está funcionando quantas vezes for necessário?
- Você tem um plano de recuperação de dados no caso de uma vulnerabilidade ser explorada?

# AMEAÇAS, VULNERABILIDADES E RISCO

## Risco

- Risco é definido como o **potencial** de perda ou dano quando uma ameaça explora uma vulnerabilidade. Exemplos de risco incluem perdas financeiras, perda de privacidade, danos à reputação, implicações legais e até perda de vidas.
- O risco também pode ser definido da seguinte forma:
- *Risco = vulnerabilidade de ameaça* X
- Reduza seu potencial de risco criando e implementando um plano de gerenciamento de riscos . Aqui estão os principais aspectos a serem considerados ao desenvolver sua estratégia de gerenciamento de riscos:

- **Avalie o risco e determine as necessidades** . Quando se trata de projetar e implementar uma estrutura de avaliação de riscos, é fundamental priorizar as violações mais importantes que precisam ser tratadas. Embora a frequência possa diferir em cada organização, esse nível de avaliação deve ser feito regularmente e de forma recorrente.
- **Inclua uma perspectiva total das partes interessadas** . As partes interessadas incluem os empresários, funcionários, clientes e até fornecedores. Todos esses atores têm o potencial de impactar negativamente a organização (ameaças em potencial), mas ao mesmo tempo podem ser ativos para ajudar a mitigar os riscos.
- **Designe um grupo central de funcionários** responsáveis pelo gerenciamento de riscos e determine o nível de financiamento apropriado para esta atividade.
- **Implemente políticas apropriadas e controles relacionados** e garanta que os usuários finais apropriados sejam informados de toda e qualquer alteração.
- **Monitorar e avaliar a eficácia da política e controle** . As fontes de risco estão sempre mudando, o que significa que sua equipe deve estar preparada para fazer os ajustes necessários na estrutura. Isso também pode envolver a incorporação de novas ferramentas e técnicas de monitoramento.

# AMEAÇAS DE REDES

- **Ameaças Internas:** Funcionário insatisfeito ou usuário mal treinado;
- **Ameaças Externas:** Ataques de cibercriminosos ou espionagem industrial;
- **Ameaças não estruturadas:** Ameaças que tem um foco geral, não necessariamente à sua empresa, mas por não implementar as boas práticas de segurança, foi afetado;
- **Ameaças estruturadas:** São ameaças que já tem um especialização, seja atacar empresas de um determinado ramo ou uma única organização;

# TIPOS DE VULNERABILIDADES EM REDES

- Utilização de protocolos de redes inseguros, Ex: FTP, HTTP, TELNET e etc;
- Sistemas operacionais vulneráveis;
- Dispositivos de redes vulnerável, sem autenticação ou com alguma vulnerabilidade;
- Serviços mal configurados;
- Utilização de senhas padrões;
- Falta de implementação de mecanismos de segurança em protocolos e dispositivos;
- Arquitetura de redes mal implementada

# ATAQUES DE REDES

- DoS e DDoS;
- Sniffing and Spoofing;
- Port Scannings;
- Malware and Viruses;
- Vulnerability Exploitation;
- Session Hijacking;
- Social Engineering;
- Envenenamento de protocolos;
- Buffer Overflow;
- Password Attacks;

https://www.bitlyft.com/what-is-computer-network-defense-cnd/

https://blog.rsisecurity.com/top-10-network-security-threats/

https://securitytrails.com/blog/top-10-common-network-security-threats-explained

https://www.cynet.com/cyber-attacks/network-attacks-and-network-security-threats/#:~:text=A%20network%20attack%20is%20an,or%20perform%20other%20malicious%20activity.&text=Passive%3A%20Attackers%20gain%20access%20to,the%20data%2C%20leaving%20it%20intact.

# NORMAS E PADRÕES

- **ISO 27001:** A norma ISO 27001 é o padrão e a referência Internacional para a gestão da Segurança da informação, assim como a ISO 9001 é a referência Internacional para a certificação de gestão em Qualidade.

  A norma ISO 27001 tem vindo, de forma continuada, a ser melhorada ao longo dos anos e deriva de um conjunto anterior de normas, nomeadamente a ISO 27001 e a BS7799 (British Standards). A sua origem remota na realidade a um documento publicado em 1992 por um departamento do governo Britânico que estabelecia um código de práticas relativas à gestão da Segurança da Informação.
  https://www.27001.pt/

- **NIST:** O National Institute of Standards and Technology (NIST) (em português: Instituto Nacional de Padrões e Tecnologia), anteriormente conhecido como The National Bureau of Standards, é uma agência governamental não regulatória da administração de tecnologia do Departamento de Comércio dos Estados Unidos. A missão do instituto é promover a inovação e a competitividade industrial dos Estados Unidos, promovendo a metrologia, os padrões e a tecnologia de forma que ampliem a segurança econômica e melhorem a qualidade de vida.

  https://www.nist.gov/

# NORMAS E PADRÕES

- **C2M2:** O programa Modelo de Maturidade em Cibersegurança (C2M2) é um esforço de parceria público-privada que foi estabelecido como resultado dos esforços da Administração para melhorar os recursos de segurança cibernética do subsetor de eletricidade e para entender a postura de segurança cibernética da rede. O C2M2 ajuda as organizações - independentemente do tamanho, tipo ou setor - a avaliar, priorizar e melhorar seus próprios recursos de segurança cibernética.
- O modelo concentra-se na implementação e gerenciamento de práticas de segurança cibernética associadas à operação e uso de ativos de tecnologia da informação e tecnologia operacional e aos ambientes em que eles operam. O objetivo é apoiar o desenvolvimento e a medição contínuos dos recursos de segurança cibernética em qualquer organização

https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0

- **PCI-DSS**: PCI DSS, acrônimo para *Payment Card Industry Data Security Standards* (Padrão de Segurança de Dados da Indústria de Cartões de Pagamento), é um padrão que prevê a proteção da privacidade e da confidencialidade da dados de cartões de pagamento. A conformidade ao PCI DSS é requerida de qualquer organização que transmita, processe ou armazene tais dados. Organizações que sofram com vazamentos de tais dados podem ter que arcar com milhões de dólares em multas e custos de remediação, perder a confiança de clientes, e sofrer com danos duradouros em suas marcas.

https://pt.pcisecuritystandards.org/index.php

# NORMAS E PADRÕES

- **HIPAA:** A Lei de Portabilidade e Responsabilidade do Seguro de Saúde de 1996 (HIPAA) exigia que o Secretário do Departamento de Saúde e Serviços Humanos dos EUA (HHS) desenvolvesse regulamentos que protegessem a privacidade e a segurança de determinadas informações de saúde.

https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

- **PTES:** O padrão de execução do teste de penetração consiste em sete (7) seções principais. Elas abrangem tudo relacionado a um teste de penetração - desde a comunicação inicial e o raciocínio por trás de um teste, até as fases de coleta de inteligência e modelagem de ameaças, nas quais os testadores estão trabalhando nos bastidores para entender melhor a organização testada, através da pesquisa de vulnerabilidades, exploração e pós-exploração, onde os conhecimentos técnicos de segurança dos testadores passam a ser combinados com o entendimento comercial do trabalho e, finalmente, com os relatórios, que capturam todo o processo, de uma maneira que faça sentido para o cliente e forneça o mais valor para isso.

http://www.pentest-standard.org/index.php/Main_Page

# NORMAS E PADRÕES

- **HIPAA:** A Lei de Portabilidade e Responsabilidade do Seguro de Saúde de 1996 (HIPAA) exigia que o Secretário do Departamento de Saúde e Serviços Humanos dos EUA (HHS) desenvolvesse regulamentos que protegessem a privacidade e a segurança de determinadas informações de saúde.

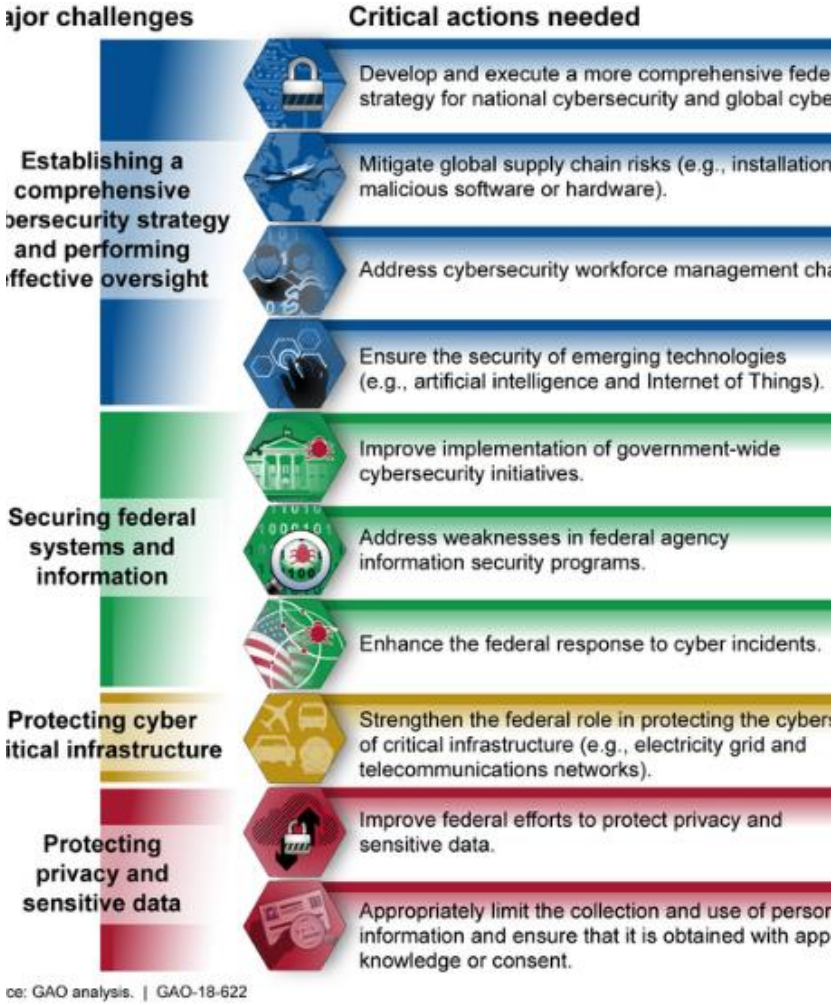
https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

- **PTES:** O padrão de execução do teste de penetração consiste em sete (7) seções principais. Elas abrangem tudo relacionado a um teste de penetração - desde a comunicação inicial e o raciocínio por trás de um teste, até as fases de coleta de inteligência e modelagem de ameaças, nas quais os testadores estão trabalhando nos bastidores para entender melhor a organização testada, através da pesquisa de vulnerabilidades, exploração e pós-exploração, onde os conhecimentos técnicos de segurança dos testadores passam a ser combinados com o entendimento comercial do trabalho e, finalmente, com os relatórios, que capturam todo o processo, de uma maneira que faça sentido para o cliente e forneça o mais valor para isso.

http://www.pentest-standard.org/index.php/Main_Page

# DESENVOLVIMENTO DE POLITICAS E RELATÓRIOS

- **Exemplos de Relatórios:** https://github.com/CyberSecurityUP/information-security-relatory
- Desenvolver um relatório e politica é essencial para priorizar e manter os devidos controles de segurança, por isso, caso tenha dúvidas, veja exemplos de como criar seu próprio report
- https://www.whitesourcesoftware.com/developers-security-report/



# MÉTODOS DE PROTEÇÕES E SEGURANÇA

# HARDENING

- **Hardening** é um processo de mapeamento das ameaças, mitigação dos riscos e execução das atividades corretivas, com foco na infraestrutura e objetivo principal de torná-la preparada para enfrentar tentativas de ataque.
- O fortalecimento de sistemas exige uma abordagem metódica para auditar, identificar, fechar e controlar possíveis vulnerabilidades de segurança em toda a organização. Existem vários tipos de atividades de proteção do sistema, incluindo:
- Endurecimento de aplicação
- Proteção do sistema operacional
- Proteção do servidor
- Proteção de banco de dados
- Proteção de rede

# HARDENING

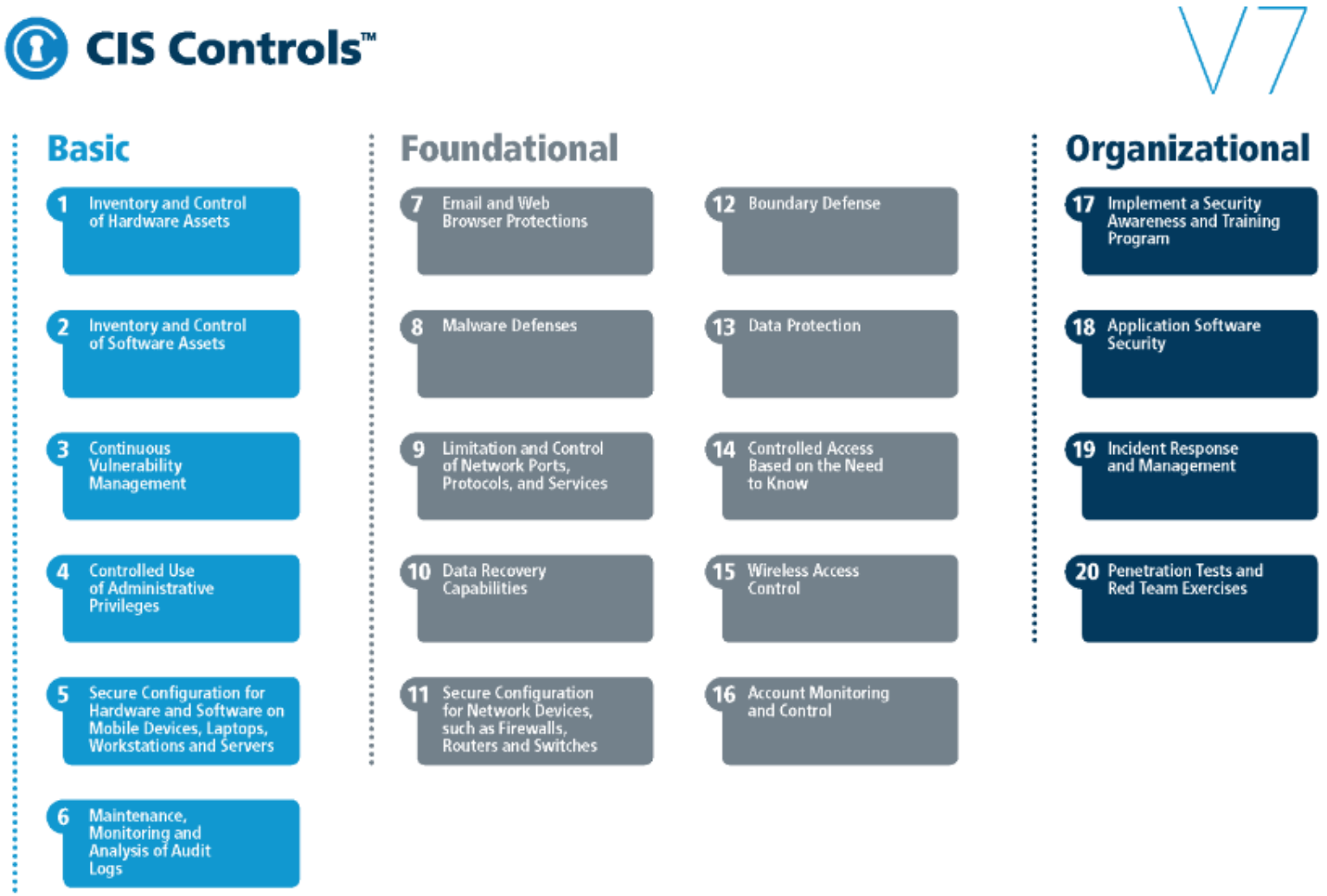
- A "superfície de ataque" é a combinação de todas as possíveis falhas e backdoors na tecnologia que podem ser exploradas por hackers. Essas vulnerabilidades podem ocorrer de várias maneiras, incluindo:
- Senhas padrão e codificadas permanentemente
- Senhas e outras credenciais armazenadas em arquivos de texto sem formatação
- Vulnerabilidades de software e firmware não corrigidas
- BIOS, firewalls, portas, servidores, comutadores, roteadores ou outras partes da infraestrutura mal configurados
- Tráfego de rede não criptografado ou dados em repouso
- Falta de acesso privilegiado

https://www.beyondtrust.com/resources/glossary/systems-hardening#:~:text=Training-,Systems%20Hardening,%2C%20firmware%2C%20and%20other%20areas.&text=By%20removing%20superfluous%20programs%2C%20accounts,%2C%20permissions%2C%20access%2C%20etc.

# CIS CONTROLS

- Os controles críticos de segurança da CIS são um conjunto recomendado de ações para defesa cibernética que fornecem maneiras específicas e acionáveis para interromper os ataques mais comuns e perigosos da atualidade. Um dos principais benefícios dos Controles é que eles priorizam e concentram um número menor de ações com altos resultados de pagamento. Os controles são eficazes porque são derivados dos padrões de ataque mais comuns destacados nos principais relatórios de ameaças e analisados em uma comunidade muito ampla de profissionais do governo e da indústria. Eles foram criados pelas pessoas que sabem como os ataques funcionam - equipes NSA Red e Blue, laboratórios de energia nuclear do Departamento de Energia dos EUA, organizações policiais e algumas das principais organizações forenses e de resposta a incidentes do país - para responder à pergunta "o que fazer precisamos fazer para impedir ataques conhecidos ". Esse grupo de especialistas chegou a um consenso e hoje temos os controles mais atuais. A chave para o valor contínuo é que os controles são atualizados com base em novos ataques que são identificados e analisados por grupos da Verizon à Symantec, para que os controles possam interromper ou atenuar esses ataques.

https://www.sans.org/critical-security-controls/




# 20 CONTROLES DO CIS

# 20 CONTROLES DO CIS - APLICADOS

- Esses 20 Controles de segurança aplicados em cima soluções
- https://www.sans.org/media/critical-security-controls/Poster_Fall_2014_CSCs_WEB.PDF

# AAA (AUTENTICAÇÃO, AUTORIZAÇÃO E AUDITORIA)

**Autenticação (Authentication)**

- A autenticação se refere ao processo de se apresentar uma identidade digital de uma entidade para outra. Normalmente, esta autenticação ocorre entre um cliente e um servidor. De uma forma mais geral, a autenticação é efetuada através da apresentação de uma identidade e suas credenciais correspondentes, como a senha associada, tickets, tokens e certificados digitais.

**Autorização (Authorization)**

- A autorização se refere à associação de certos tipos de privilégios para uma entidade, baseados na própria autenticação da entidade e de quais serviços estão sendo requisitados. Dentre as políticas de autorização, podemos utilizar restrições em determinados horários, restrições de acordo com o grupo ao qual pertence o usuário e proteção contra múltiplas conexões simultâneas efetuadas pelo mesmo usuário. Como exemplo de aplicações que utilizam estas políticas de autorização, podemos citar as políticas de Qualidade de Serviço, que podem fornecer mais banda de acordo com o serviço requisitado, o controle de certos tipos de pacotes, como ocorre no traffic shapping, dentre outros.

**Auditoria (Accounting)**

- Accounting se refere ao monitoramento do comportamento dos usuários e de que forma estes consomem os recursos da rede. Estas informações podem ser muito úteis para melhor gerenciar os recursos de rede, para a cobrança de serviços e para o planejamento de quais setores da rede precisam ser melhorados.

https://www.gta.ufrj.br/grad/08_1/radius/Auditoria(Accounting).html#Topic13

# TIPOS DE AUTENTICAÇÃO

**Autenticação de fator único**

- Também conhecida como autenticação primária , essa é a forma mais simples e comum de autenticação. A autenticação de fator único requer, é claro, apenas um método de autenticação, como senha, pino de segurança, cartão PIV etc. para conceder acesso a um sistema ou serviço.

**Autenticação de 2º fator**

- Adicionando uma camada de complexidade, o 2FA requer um segundo fator para verificar a identidade do usuário. Exemplos comuns incluem tokens gerados por um dispositivo registrado, senhas de uso único ou números PIN. A mera presença de dois métodos de autenticação melhora significativamente sua postura de segurança - de fato, de acordo com uma pesquisa da Symantec , **80% das violações de dados podem ser evitadas pelo 2FA.**

# TIPOS DE AUTENTICAÇÃO

**Autenticação multifatorial**

- A autenticação multifator (MFA) é o método de autenticação mais sofisticado que utiliza 2 ou mais fatores independentes para conceder acesso do usuário a um sistema. Em cenários típicos, os métodos de AMF aproveitam pelo menos 2 ou 3 das seguintes categorias.

1. **Algo que você sabe** - uma senha ou um alfinete
2. **Algo que você tem** - telefone celular ou um token de segurança
3. **Algo que você é** - impressão digital ou FaceID
4. **Algo que você faz** - velocidade de digitação, informações de localização etc.

**Autenticação básica HTTP**

- Usando essa abordagem, um agente de usuário simplesmente fornece um nome de usuário e senha para provar sua autenticação. Essa abordagem não requer cookies, IDs de sessão ou páginas de login porque utiliza o próprio cabeçalho HTTP. Embora simples de usar, esse método de autenticação é vulnerável a ataques que podem capturar as credenciais do usuário em trânsito.

# TIPOS DE AUTENTICAÇÃO

**Chaves de API**

- Uma chave de API é um identificador destinado a identificar a origem das solicitações de serviço da web (ou tipos semelhantes de solicitações). Uma chave é gerada na primeira vez que um usuário tenta obter acesso autorizado a um sistema através do registro. A partir daí, a chave da API se associa a um token secreto e é enviada juntamente com as solicitações posteriores. Quando o usuário tenta entrar novamente no sistema, sua chave exclusiva é usada para provar que é o mesmo usuário de antes. Este método de autenticação da API é muito rápido e confiável, mas é frequentemente mal utilizado. Mais importante, esse método de autenticação não é um método de autorização.

**OAuth**

- Oauth é um dos métodos mais seguros de autenticação de API e suporta autenticação e autorização. OAuth permite que a API seja autenticada estabelecendo escopo e pode acessar o sistema ou recurso solicitado. Este é fundamentalmente um meio muito seguro de autenticação na sua API.

https://www.okta.com/blog/2019/02/the-ultimate-authentication-playbook/

# PROTOCOLOS DE SEGURANÇA DE REDES

- SSH, SFTP, HTTPS, SSL, TLS, WPA2, IPSEC e etc
- https://crypto.stanford.edu/cs155old/cs155-spring11/lectures/13-network-defense.pdf
- https://www.ibm.com/support/knowledgecenter/SSLTBW_2.4.0/com.ibm.zos.v2r4.halz002/security_protocols.htm
- https://enterprisedt.com/white-papers/how_ssh_tls_sftp_and_ftps_work.pdf

# CERTIFICADO DIGITAL

- Um **Certificado Digital** é uma "senha" eletrônica que permite a uma organização organizar troca de dados com segurança pela Internet usando a infraestrutura de chave pública (PKI). O certificado digital também é conhecido como **certificado de chave pública** ou **certificado de identidade.**
- Um certificado Digital possui:
  - Detalhes de chave pública do proprietário
  - Nome do Proprietário
  - Data de expiração da chave pública
  - Nome da Autoridade Certificadora (CA)
  - Número de série do Certificado
  - Assinatura digital do Emissor

https://www.digicert.com/ssl/

https://www.comodo.com/resources/small-business/digital-certificates.php

https://en.wikipedia.org/wiki/Public_key_certificate

https://pt.wikipedia.org/wiki/Certificado_digital

# GESTÃO DE PATCHES

- O gerenciamento de patches é o processo que ajuda a adquirir, testar e instalar vários patches (alterações de código) em aplicativos e ferramentas de software existentes em um computador, permitindo que os sistemas se mantenham atualizados sobre os patches existentes e determinando quais são os apropriados. O gerenciamento de patches se torna fácil e simples.
- O gerenciamento de patches é feito principalmente por empresas de software como parte de seus esforços internos para corrigir problemas com as diferentes versões de programas de software e também para ajudar a analisar programas de software existentes e detectar qualquer possível falta de recursos de segurança ou outras atualizações.
- **As correções de software** ajudam a corrigir os problemas existentes e são notados somente após o lançamento inicial do software. Os patches referem-se principalmente à segurança, enquanto existem alguns que também dizem respeito à funcionalidade específica dos programas.

https://www.itarian.com/patch-management.php

# GESTÃO DE VULNERABILIDADES

- O gerenciamento de vulnerabilidades é uma responsabilidade essencial de qualquer equipe de segurança de TI ou provedor de serviços de segurança gerenciado , e envolve a avaliação, a atenuação (se necessário) e o relatório de quaisquer vulnerabilidades de segurança existentes nos sistemas e software de uma organização. Porém, as vulnerabilidades podem ser gerenciadas apenas se forem descobertas e identificadas, e a maneira de conseguir isso é através de um programa abrangente de verificação de vulnerabilidades.

https://www.esecurityplanet.com/network-security/vulnerability-scanning.html

# ANALISE DE VULNERABILIDADE

- A verificação de vulnerabilidades e os testes de penetração costumam ser confusos, mas, na verdade, os dois procedimentos de segurança são bem diferentes e são usados para propósitos diferentes.
- No nível mais básico, a verificação de vulnerabilidades visa identificar quaisquer sistemas sujeitos a vulnerabilidades conhecidas, enquanto um teste de penetração visa identificar pontos fracos nas configurações específicas do sistema e nos processos e práticas organizacionais que podem ser explorados para comprometer a segurança.
- Como ilustração da diferença entre uma verificação de vulnerabilidade e um teste de penetração, um teste de caneta pode envolver:
- Usando técnicas de engenharia social , como se passar por um gerente e pedir uma senha a um funcionário para obter acesso a um banco de dados ou outro sistema
- Interceptando e usando senhas não criptografadas enviadas pela rede
- Enviar e-mails de phishing para usuários para obter acesso a contas

# ANALISE DE VULNERABILIDADE

- A verificação de vulnerabilidades localiza sistemas e software que possuem vulnerabilidades de segurança conhecidas, mas essas informações são úteis apenas para as equipes de segurança de TI quando usadas como a primeira parte de um processo de gerenciamento de vulnerabilidades em quatro partes.
- **Processo de gerenciamento de vulnerabilidades**
- Esse processo de gerenciamento de vulnerabilidades envolve:
- Identificação de vulnerabilidades
- Avaliação do risco representado por quaisquer vulnerabilidades identificadas
- Tratamento de quaisquer vulnerabilidades identificadas
- Relatórios sobre vulnerabilidades e como elas foram tratadas

# ANALISE DE VULNERABILIDADE

- **Identificação de vulnerabilidades**
- A principal maneira de identificar vulnerabilidades é através da verificação de vulnerabilidades, e a eficácia de um scanner depende de duas coisas:
- a capacidade do scanner de localizar e identificar dispositivos, software e portas abertas e coletar outras informações do sistema
- a capacidade de correlacionar essas informações com informações conhecidas sobre vulnerabilidade de um ou mais bancos de dados de vulnerabilidade
- A verificação de vulnerabilidade pode ser configurada para ser mais ou menos agressiva ou invasiva, e isso é importante porque existe a possibilidade de que o processo de verificação possa afetar o desempenho ou a estabilidade dos sistemas que estão sendo interrogados. Também pode causar problemas de largura de banda em algumas redes.

https://www.esecurityplanet.com/network-security/vulnerability-scanning.html

# CONTROLES DE SEGURANÇA

- A segurança do computador geralmente é dividida em três categorias principais distintas, comumente chamadas de *controles* :
- Fisica
- Técnico
- Administrativo
- Essas três categorias amplas definem os principais objetivos da implementação de segurança adequada. Dentro desses controles, existem subcategorias que detalham mais os controles e como implementá-los.

# CONTROLES DE SEGURANÇA

**Controles Físicos**

- Controle físico é a implementação de medidas de segurança em uma estrutura definida usada para impedir ou impedir o acesso não autorizado a materiais sensíveis. Exemplos de controles físicos são:
- Câmeras de vigilância em circuito fechado
- Sistemas de alarme térmico ou de movimento
- Seguranças
- Pictures IDs
- Portas de aço trancadas e parafusadas
- Biometria (inclui impressão digital, voz, rosto, íris, caligrafia e outros métodos automatizados usados para reconhecer indivíduos)

# CONTROLES DE SEGURANÇA

**Controles Técnicos**

- Os controles técnicos usam a tecnologia como base para controlar o acesso e o uso de dados confidenciais em uma estrutura física e em uma rede. Os controles técnicos têm amplo alcance e abrangem tecnologias como:
- Criptografia
- Cartões inteligentes
- Autenticação de rede
- Listas de controle de acesso (ACLs)
- Software de auditoria de integridade de arquivos

# CONTROLES DE SEGURANÇA

**Controles Administrativos**

- Os controles administrativos definem os fatores humanos de segurança. Envolve todos os níveis de pessoal dentro de uma organização e determina quais usuários têm acesso a quais recursos e informações por meios como:
- Treinamento e conscientização
- Planos de preparação e recuperação de desastres
- Estratégias de recrutamento e separação de pessoal
- Registro e contabilidade de pessoal

# FIREWALLS

- Um firewall é um dispositivo de segurança da rede que monitora o tráfego de rede de entrada e saída e decide permitir ou bloquear tráfegos específicos de acordo com um conjunto definido de regras de segurança.
- Os firewalls têm sido a linha de frente da defesa na segurança de rede há mais de 25 anos. Eles colocam uma barreira entre redes internas protegidas e controladas que podem ser redes externas confiáveis ou não, como a Internet.
- Um firewall pode ser um hardware, software ou ambos.

# FIREWALLS - TIPOS

- Os tipos de firewall podem ser divididos em várias categorias diferentes, com base em sua estrutura geral e método de operação. Aqui estão oito tipos de firewalls :

1. Firewalls de filtragem de pacotes
2. Gateways no nível do circuito
3. Firewalls de inspeção com estado
4. Gateways no nível do aplicativo (aka firewalls proxy)
5. Firewalls de última geração
6. Firewalls de software
7. Firewalls de hardware
8. Firewalls na nuvem

https://www.compuquip.com/blog/the-different-types-of-firewall-architectures

https://searchsecurity.techtarget.com/feature/The-five-different-types-of-firewalls

https://medium.com/@shrinathdhormare/what-is-firewall-1d978072 1e9a

# VPN

- Uma VPN, ou rede virtual privada, permite criar uma conexão segura com outra rede pela Internet. As VPNs podem ser usadas para acessar sites restritos por região, proteger sua atividade de navegação de olhares indiscretos no Wi-Fi público e muito mais.
- Em termos muito simples, uma VPN conecta seu PC, smartphone ou tablet a outro computador (chamado servidor) em algum lugar da Internet e permite navegar na Internet usando a conexão à Internet desse computador. Portanto, se esse servidor estiver em um país diferente, parecerá que você é proveniente desse país e poderá acessar coisas que normalmente não poderia.
- Então, como isso ajuda você? Boa pergunta! Você pode usar uma VPN para:
- Ignore restrições geográficas em sites ou faça streaming de áudio e vídeo.
- Assista a streaming de mídia como Netflix e Hulu.
- Proteja-se de bisbilhotar pontos de acesso Wi-Fi não confiáveis.
- Obtenha pelo menos algum anonimato online ocultando sua verdadeira localização.
- Proteja-se contra o logon durante o torrent.
- Atualmente, muitas pessoas estão usando uma VPN para torrent ou contornar restrições geográficas para assistir a conteúdo em um país diferente. Eles ainda são muito úteis para se proteger enquanto trabalha em uma cafeteria, mas esse dificilmente é o único uso.

https://www.howtogeek.com/133680/htg-explains-what-is-a-vpn/

# VPN - PROTOCOLOS

- Existem duas abordagens principais para a funcionalidade VPN: 1) dois protocolos são usados (um protocolo para mover os dados pelo túnel e um protocolo para proteger esse tráfego); ou 2) um protocolo é usado para transferência e segurança de dados.
- Aqui estão cinco protocolos VPN comuns e seus principais benefícios.
- **1) PPTP**
  O protocolo de encapsulamento ponto a ponto PPTP é um dos protocolos VPN mais antigos existentes. Desenvolvido em meados dos anos 90 pela Microsoft , o PPTP foi integrado ao Windows 95 e projetado especificamente para conexões dial-up. Porém, com o avanço da tecnologia, a criptografia básica do PPTP foi rapidamente quebrada, comprometendo sua segurança subjacente. No entanto, como carece de muitos dos recursos de segurança encontrados em outros protocolos modernos, ele pode oferecer as melhores velocidades de conexão para usuários que talvez não precisem de criptografia pesada. Porém, embora o PPTP ainda seja usado em alguns aplicativos, a maioria dos provedores já atualizou para protocolos mais rápidos e confiáveis.

# VPN - PROTOCOLOS

- **2) L2TP/IPSEC**
  protocolo de túnel **L2TP / IPSec** Layer 2 é uma substituição do protocolo VPN PPTP. Este protocolo não fornece nenhuma criptografia ou privacidade pronta para uso e é frequentemente emparelhado com o protocolo de segurança IPsec. Uma vez implementado, o L2TP / IPsec é extremamente seguro e não possui vulnerabilidades conhecidas.
- **3) OpenVPN**
  OpenVPN é um protocolo de código aberto que permite que os desenvolvedores acessem seu código subjacente. Esse protocolo cresceu em popularidade devido ao uso de criptografia de chave AES-256 bits (praticamente inquebrável) com autenticação RSA de 2048 bits e um algoritmo de hash SHA1 de 160 bits.
- **4) SSTP**
  protocolo **SSTP** Secure Socket Tunneling é popular devido à sua total integração com todos os sistemas operacionais da Microsoft desde o Windows Vista SP 1. O SSTP utiliza certificados SSL / TLS de 2048 bits para autenticação e chaves SSL de 256 bits para criptografia. A maior desvantagem do SSTP é que ele é basicamente um protocolo proprietário desenvolvido pela Microsoft e os desenvolvedores não têm acesso ao código subjacente.

# VPN - PROTOCOLOS

- **5)IKEv2**
  A versão 2 do **IKEv2** Internet Key Exchange é um protocolo de encapsulamento de VPN comum que fornece uma sessão segura de troca de chaves. Semelhante ao L2TP (e IKEv1), o IKEv2 normalmente é associado ao IPsec para criptografia e autenticação. Esse protocolo é muito bom para restabelecer o link após perda temporária de conexão e se destaca na troca de conexões entre tipos de rede (de WiFi a celular, por exemplo).

https://www.netmotionsoftware.com/blog/connectivity/vpn-protocols

# PROXY

- Um servidor proxy atua como um gateway entre você e a Internet. É um servidor intermediário que separa os usuários finais dos sites em que navegam. Os servidores proxy fornecem níveis variados de funcionalidade, segurança e privacidade, dependendo do seu caso de uso, necessidades ou política da empresa.
- Se você estiver usando um servidor proxy, o tráfego da Internet fluirá pelo servidor proxy no caminho para o endereço solicitado. A solicitação volta pelo mesmo servidor proxy (há exceções a essa regra) e, em seguida, o servidor proxy encaminha os dados recebidos do site para você.
- Os servidores proxy modernos fazem muito mais do que encaminhar solicitações da Web, tudo em nome da segurança dos dados e do desempenho da rede. Os servidores proxy agem como um firewall e um filtro da web, fornecem conexões de rede compartilhadas e armazenam dados em cache para acelerar solicitações comuns. Um bom servidor proxy mantém os usuários e a rede interna protegidos das coisas ruins que existem na Internet selvagem. Por fim, os servidores proxy podem fornecer um alto nível de privacidade.

# PROXY

- Existem várias razões pelas quais as organizações e os indivíduos usam um servidor proxy.
- **Para controlar o uso da Internet de funcionários e filhos:** Organizações e pais configuram servidores proxy para controlar e monitorar como seus funcionários ou filhos usam a Internet. A maioria das organizações não deseja que você procure sites específicos no horário da empresa e pode configurar o servidor proxy para negar o acesso a sites específicos, em vez disso, redirecionando-o com uma nota legal solicitando que você evite consultar os sites na rede da empresa. Eles também podem monitorar e registrar todas as solicitações da Web; portanto, mesmo que não possam bloquear o site, eles sabem quanto tempo você gasta no cyberloaf.
- **Economia de largura de banda e velocidades aprimoradas: as** organizações também podem obter melhor desempenho geral da rede com um bom servidor proxy. Os servidores proxy podem armazenar em cache (salvar uma cópia do site localmente) sites populares - portanto, quando você solicitar www.varonis.com , o servidor proxy verificará se possui a cópia mais recente do site e enviará o cópia salva. O que isso significa é que, quando centenas de pessoas acessam www.varonis.com ao mesmo tempo no mesmo servidor proxy, o servidor proxy envia apenas uma solicitação ao varonis.com. Isso economiza largura de banda para a empresa e melhora o desempenho da rede.
- **Benefícios de privacidade:** indivíduos e organizações usam servidores proxy para navegar na Internet de maneira mais privada. Alguns servidores proxy alteram o endereço IP e outras informações de identificação contidas na solicitação da web. Isso significa que o servidor de destino não sabe quem realmente fez a solicitação original, o que ajuda a manter suas informações pessoais e hábitos de navegação mais privados.

# PROXY

- **Segurança aprimorada:** Os servidores proxy oferecem benefícios de segurança além dos benefícios de privacidade. Você pode configurar seu servidor proxy para criptografar suas solicitações da web para impedir que olhares curiosos leiam suas transações. Você também pode impedir sites de malware conhecidos de qualquer acesso através do servidor proxy. Além disso, as organizações podem associar seu servidor proxy a uma rede virtual privada (VPN), para que os usuários remotos sempre acessem a Internet por meio do proxy da empresa. Uma VPN é uma conexão direta com a rede da empresa que as empresas fornecem a usuários externos ou remotos. Ao usar uma VPN, a empresa pode controlar e verificar se seus usuários têm acesso aos recursos (email, dados internos) de que precisam, além de fornecer uma conexão segura para o usuário proteger os dados da empresa.
- **Obtenha acesso a recursos bloqueados: os** servidores proxy permitem que os usuários contornem as restrições de conteúdo impostas por empresas ou governos. O jogo da equipe de sportsball local está bloqueado online? Faça login em um servidor proxy no outro lado do país e assista a partir daí. O servidor proxy faz com que pareça que você está na Califórnia, mas na verdade mora na Carolina do Norte. Vários governos ao redor do mundo monitoram e restringem de perto o acesso à Internet, e os servidores proxy oferecem aos cidadãos acesso a uma Internet sem censura.

https://www.varonis.com/blog/what-is-a-proxy-server/

# IDS E IPS

- Os Sistemas de Detecção de Intrusão (IDS) analisam o tráfego da rede em busca de assinaturas que correspondam a ciberataques conhecidos. Os Sistemas de Prevenção de Intrusões (IPS) também analisam pacotes, mas podem impedir que esses pacotes sejam entregues com base nos tipos de ataques detectados – ajudando a interromper o ataque.
- A principal diferença entre eles é que o IDS é um sistema de monitoramento, enquanto o IPS é um sistema de controle.
- O IDS não altera os pacotes de rede de nenhuma maneira, já o IPS impede que o pacote seja entregue com base em seu conteúdo, da mesma forma como um firewall impede o tráfego por endereço IP.
- Sistemas de Detecção de Invasão (IDS): analisa e monitora o tráfego da rede em busca de sinais indicando que invasores estão usando uma ameaça conhecida para se infiltrar e roubar dados da rede. Os sistemas IDS comparam a atividade da rede atual a um banco de dados de ameaças conhecida para detectar vários tipos de comportamento, como violações de políticas de segurança, malware e verificações de portas.
- Sistemas de Prevenção de Intrusões (IPS) Vivem na mesma área da rede que um firewall, entre o mundo externo e a rede interna. O IPS nega proativamente o tráfego de rede com base em um perfil de segurança, se esse pacote representar uma ameaça de segurança conhecida.

# IDS E IPS

- Ambos leem pacotes de rede e comparam o conteúdo a um banco de dados de ameaças conhecidas. A principal diferença entre eles é o que acontece a seguir. Os IDSs são ferramentas de detecção e monitoramento que não agem por conta própria. Os IPSs são sistemas de controle que aceitam ou rejeitam um pacote baseado em um conjunto de regras.
- O IDS exige que um ser humano, ou outro sistema, analise os resultados e determine quais ações tomar em seguida, o que pode ser um trabalho em tempo integral, dependendo da quantidade de tráfego de rede gerada a cada dia. O propósito do IPS, por outro lado, é pegar pacotes perigosos e barrá-los antes que eles atinjam o alvo. É mais passivo que um IDS, exigindo apenas que o banco de dados seja atualizado regularmente com novos dados de ameaças.

https://blog.varonis.com.br/ids-vs-ips-qual-a-diferenca/

# NIDS, HIDS E WIDS

- **HIDs** : Os sistemas de detecção de intrusões de host são um tipo de gerenciamento de segurança para seus computadores e redes. Utilizando firewalls, software antivírus e programas de detecção de spyware, esses aplicativos anti-ameaças são instalados nos **computadores** da **rede** com acesso bidirecional - por exemplo, a Internet.
- **NIDs** : Os sistemas de detecção de intrusão de rede são um tipo de gerenciamento de segurança para seus computadores e redes. No entanto, os firewalls, o software antivírus e os programas de detecção de spyware que compõem os NIDs são instalados em pontos específicos - como **servidores** - que funcionam entre o ambiente externo (pense na Internet) e o segmento de rede a ser protegido (os servidores).
- **WIDs** : Os sistemas sem fio de detecção de intrusões são interessantes, pois detectam ataques de redes prejudiciais, **examinando o espectro de rádio em** busca de pontos de acesso não autorizados e agindo.

https://www.neovera.com/hids-nids-wids/

# CRIPTOGRAFIAS

- A criptografia é uma técnica de proteção de informações e comunicações por meio do uso de códigos, para que somente as pessoas a quem as informações são destinadas possam entendê-las e processá-las. Impedindo assim o acesso não autorizado a informações. O prefixo "cripta" significa "oculto" e grafia com sufixo significa "escrita".
- Na criptografia, as técnicas usadas para proteger as informações são obtidas de conceitos matemáticos e de um conjunto de cálculos baseados em regras, conhecidos como algoritmos, para converter mensagens de maneira a dificultar a decodificação. Esses algoritmos são usados para geração de chave criptográfica, assinatura digital, verificação para proteger a privacidade dos dados, navegação na Internet e para proteger transações confidenciais, como transações com cartão de crédito e cartão de débito.

**Tipos de criptografia:**

1. **Criptografia de chave simétrica:**
   é um sistema de criptografia em que o remetente e o destinatário da mensagem usam uma única chave comum para criptografar e descriptografar mensagens. Os sistemas de chave simétrica são mais rápidos e simples, mas o problema é que o remetente e o destinatário precisam, de alguma forma, trocar a chave de maneira segura. O sistema de criptografia de chave simétrica mais popular é o Sistema de Criptografia de Dados (DES).
2. **Funções de hash:**
   Não há uso de nenhuma chave nesse algoritmo. Um valor de hash com comprimento fixo é calculado de acordo com o texto sem formatação, o que torna impossível a recuperação do conteúdo do texto sem formatação. Muitos sistemas operacionais usam funções hash para criptografar senhas.
3. **Criptografia de chave assimétrica:**
   sob esse sistema, um par de chaves é usado para criptografar e descriptografar informações. Uma chave pública é usada para criptografia e uma chave privada é usada para descriptografia. Chave pública e chave privada são diferentes. Mesmo que a chave pública seja conhecida por todos, o destinatário pretendido pode decodificá-la apenas porque ele conhece a chave privada.

# CRIPTOGRAFIAS - ALGORITMOS

**1. DES triplo**

- O Triple DES foi projetado para substituir o algoritmo original do Data Encryption Standard (DES), que os hackers acabaram aprendendo a derrotar com relativa facilidade. Ao mesmo tempo, o Triple DES foi o padrão recomendado e o algoritmo simétrico mais amplamente usado na indústria.
- O DES triplo usa três chaves individuais com 56 bits cada. O comprimento total da chave soma 168 bits, mas os especialistas argumentam que 112 bits na força da chave são mais parecidos.
- Apesar de ser gradualmente eliminado, o Triple DES ainda consegue criar uma solução confiável de criptografia de hardware para serviços financeiros e outros setores.

**2. RSA**

- O RSA é um algoritmo de criptografia de chave pública e o padrão para criptografar dados enviados pela Internet. Também é um dos métodos usados em nossos programas PGP e GPG.
- Ao contrário do Triple DES, o RSA é considerado um algoritmo assimétrico devido ao uso de um par de chaves. Você tem sua chave pública, que é o que usamos para criptografar nossa mensagem, e uma chave privada para descriptografá-la. O resultado da criptografia RSA é um enorme lote de mumbo jumbo que leva aos invasores bastante tempo e poder de processamento para serem quebrados.

# CRIPTOGRAFIAS - ALGORITMOS

**3. Blowfish**

- Blowfish é outro algoritmo projetado para substituir o DES. Essa cifra simétrica divide as mensagens em blocos de 64 bits e as criptografa individualmente.
- Blowfish é conhecido por sua velocidade tremenda e eficácia geral, pois muitos afirmam que nunca foi derrotado. Enquanto isso, os fornecedores aproveitaram ao máximo sua disponibilidade gratuita em domínio público.
- O Blowfish pode ser encontrado em categorias de software, desde plataformas de comércio eletrônico para proteção de pagamentos até ferramentas de gerenciamento de senhas, onde costumava proteger senhas. É definitivamente um dos métodos de criptografia mais flexíveis disponíveis.

**4. Twofish**

- Bruce Schneier, especialista em segurança de computadores, é o cérebro por trás do Blowfish e seu sucessor, Twofish . As chaves usadas neste algoritmo podem ter até 256 bits de comprimento e, como técnica simétrica, apenas uma chave é necessária.
- O Twofish é considerado um dos mais rápidos do gênero e ideal para uso em ambientes de hardware e software. Como o Blowfish, o Twofish está disponível gratuitamente para quem quiser usá-lo. Como resultado, você o encontrará em programas de criptografia como o PhotoEncrypt, GPG e o popular software de código aberto TrueCrypt .

# CRIPTOGRAFIAS - ALGORITMOS

**5. AES**

- O Advanced Encryption Standard (AES) é o algoritmo confiável como padrão pelo governo dos EUA e por várias organizações.
- Embora seja extremamente eficiente na forma de 128 bits, o AES também usa chaves de 192 e 256 bits para fins de criptografia pesada.
- O AES é amplamente considerado impermeável a todos os ataques, com exceção da força bruta, que tenta decifrar as mensagens usando todas as combinações possíveis na cifra de 128, 192 ou 256 bits. Ainda assim, os especialistas em segurança acreditam que a AES acabará sendo aclamada pelo padrão de fato para criptografar dados no setor privado.

# CRIPTOGRAFIAS - FUNÇÃO

- As funções de hash são extremamente úteis e aparecem em quase todos os aplicativos de segurança da informação.
- Uma função hash é uma função matemática que converte um valor numérico de entrada em outro valor numérico compactado. A entrada para a função hash é de comprimento arbitrário, mas a saída é sempre de comprimento fixo.
- Os valores retornados por uma função de hash são chamados de **resumo da mensagem** ou simplesmente **valores de hash**
- Os recursos típicos das funções de hash são -
- **Saída de comprimento fixo (valor de hash)**
  - A função hash abrange dados de comprimento arbitrário para um comprimento fixo. Esse processo geralmente é chamado de **hash dos dados** .
  - Em geral, o hash é muito menor que os dados de entrada; portanto, as funções de hash são chamadas de **funções de compactação** .
  - Como um hash é uma representação menor de dados maiores, também é chamado de **resumo** .
  - A função hash com saída de n bits é chamada de **função hash de n bits** . Funções hash populares geram valores entre 160 e 512 bits. (https://www.tutorialspoint.com/cryptography/cryptography_hash_functions.htm)

Esta é uma lista de funções de hash , incluindo verificações de redundância cíclica , funções de soma de verificação e funções de hash criptográficas

https://en.wikipedia.org/wiki/List_of_hash_functions

# CRIPTOGRAFIAS – BASE64

- Base64 é um método para codificação de dados para transferência na Internet (codificação MIME para transferência de conteúdo). É utilizado frequentemente para transmitir dados binários por meios de transmissão que lidam apenas com texto, como por exemplo para enviar arquivos anexos por e-mail.
- É constituído por 64 caracteres ([A-Z],[a-z],[0-9], "/" e "+") que deram origem ao seu nome. O carácter "=" é utilizado como um sufixo especial e a especificação original (RFC 989) definiu que o símbolo "*" pode ser utilizado para delimitar dados convertidos, mas não criptografados, dentro de um stream.
- **Exemplo de codificação:**
  - Texto original: Olá, mundo!
  - Texto convertido para Base64: T2zDoSwgbXVuZG8h
- A codificação Base64 é frequentemente utilizada quando existe uma necessidade de transferência e armazenamento de dados binários para um dispositivo designado para trabalhar com dados textuais. Esta codificação é amplamente utilizada por aplicações em conjunto com a linguagem de marcação XML, possibilitando o armazenamento de dados binários em forma de texto.

https://pt.wikipedia.org/wiki/Base64

# GESTÃO DE SENHAS

- Um gerenciador de senhas é um aplicativo de software usado para armazenar e gerenciar as senhas que um usuário possui para várias contas online e recursos de segurança. Os gerenciadores de senhas armazenam as senhas em um formato criptografado e fornecem acesso seguro a todas as informações de senha com a ajuda de uma senha mestra.
- Existem muitos tipos de gerenciadores de senhas, diferindo na maneira como criptografam as informações, o tipo de armazenamento e os recursos adicionais fornecidos.
- Os gerenciadores de senhas são aplicativos que servem como a solução para manter um grande número de senhas e informações da conta. Eles armazenam as informações de login das várias contas e as inserem automaticamente nos formulários. Isso ajuda na prevenção de ataques de hackers, como registro de pressionamento de tecla, e evita a necessidade de lembrar várias senhas.
- **Alguns dos tipos:**
  - Web browser-based
  - Cloud-based
  - Desktop
  - Portable
  - Stateless

# GESTÃO DE RISCOS

- O gerenciamento de riscos é o processo de identificação, avaliação e controle de ameaças ao capital e aos ganhos de uma organização. Essas ameaças ou riscos podem resultar de uma ampla variedade de fontes, incluindo incerteza financeira, responsabilidades legais, erros de gerenciamento estratégico, acidentes e desastres naturais. As ameaças à segurança de TI e os riscos relacionados aos dados, e as estratégias de gerenciamento de riscos para aliviá-los, tornaram-se uma das principais prioridades das empresas digitalizadas . Como resultado, um plano de gerenciamento de riscos inclui cada vez mais os processos das empresas para identificar e controlar ameaças a seus ativos digitais, incluindo dados corporativos proprietários, informações de identificação pessoal (PII) de um cliente e propriedade intelectual.
- Todas as empresas e organizações correm o risco de eventos inesperados e prejudiciais que podem custar dinheiro à empresa ou causar seu fechamento permanente. O gerenciamento de riscos permite que as organizações tentem se preparar para o inesperado, minimizando riscos e custos extras antes que eles aconteçam.

# GESTÃO DE RISCOS

- Ao implementar um plano de gerenciamento de riscos e considerando os vários riscos ou eventos em potencial antes que eles ocorram, uma organização pode economizar dinheiro e proteger seu futuro. Isso ocorre porque um plano robusto de gerenciamento de riscos ajudará a empresa a estabelecer procedimentos para evitar ameaças em potencial, minimizar seu impacto caso ocorram e lidar com os resultados. Essa capacidade de entender e controlar os riscos permite que as organizações tenham mais confiança em suas decisões de negócios. Além disso, princípios sólidos de governança corporativa que se concentram especificamente no gerenciamento de riscos podem ajudar a empresa a atingir seus objetivos.
- **Outros benefícios importantes do gerenciamento de riscos incluem:**
  - Cria um ambiente de trabalho seguro para todos os funcionários e clientes.
  - Aumenta a estabilidade das operações comerciais e reduz a responsabilidade legal.
  - Oferece proteção contra eventos que são prejudiciais à empresa e ao meio ambiente.
  - Protege todas as pessoas e ativos envolvidos contra possíveis danos.
  - Ajuda a estabelecer as necessidades de seguro da organização para economizar em prêmios desnecessários.

# GESTÃO DE RISCOS

- **Todos os planos de gerenciamento de riscos seguem as mesmas etapas que se combinam para compor o processo geral de gerenciamento de riscos:**

- **Estabelecer contexto.** Entenda as circunstâncias nas quais o restante do processo ocorrerá. Os critérios que serão utilizados para avaliar o risco também devem ser estabelecidos e a estrutura da análise deve ser definida.
- **Identificação de riscos.** A empresa identifica e define riscos potenciais que podem influenciar negativamente um processo ou projeto específico da empresa.
- **Análise de risco.** Depois que tipos específicos de risco são identificados, a empresa determina as chances de ocorrência, bem como suas conseqüências. O objetivo da análise de risco é entender melhor cada instância específica de risco e como isso pode influenciar os projetos e objetivos da empresa.
- **Avaliação de riscos e avaliação.** O risco é então avaliado posteriormente após a determinação da probabilidade geral de ocorrência do risco combinada com sua consequência geral. A empresa pode então tomar decisões sobre se o risco é aceitável e se está disposto a adotá-lo com base no apetite ao risco .
- **Mitigação de riscos** . Durante esta etapa, as empresas avaliam seus riscos mais bem classificados e desenvolvem um plano para aliviá-los usando controles de risco específicos. Esses planos incluem processos de mitigação de riscos, táticas de prevenção de riscos e planos de contingência no caso de o risco se concretizar.
- **Monitoramento de riscos** . Parte do plano de mitigação inclui o acompanhamento dos riscos e do plano geral para monitorar e rastrear continuamente os riscos novos e existentes. O processo geral de gerenciamento de riscos também deve ser revisado e atualizado de acordo.
- **Comunicar e consultar.** Os acionistas internos e externos devem ser incluídos na comunicação e consulta em cada etapa apropriada do processo de gerenciamento de riscos e no processo como um todo.

# WI-FI SECURITY

- Vários protocolos de segurança sem fio foram desenvolvidos para proteger redes sem fio domésticas. Esses protocolos de segurança sem fio incluem WEP, WPA e WPA2, cada um com seus próprios pontos fortes e fracos. Além de impedir que convidados indesejados se conectem à sua rede sem fio, os protocolos de segurança sem fio criptografam seus dados privados à medida que são transmitidos pelas ondas de rádio.
- **Wired Equivalent Privacy (WEP):**o protocolo de criptografia original desenvolvido para redes sem fio. Como o próprio nome indica, o WEP foi projetado para fornecer o mesmo nível de segurança que as redes com fio. No entanto, o WEP possui muitas falhas de segurança conhecidas, é difícil de configurar e é facilmente quebrado.
- **Wi-Fi Protected Access (WPA):** Introduzido como um aprimoramento de segurança provisório via WEP enquanto o padrão de segurança sem fio 802.11i estava sendo desenvolvido. As implementações mais recentes do WPA usam uma chave pré-compartilhada (PSK), geralmente chamada de *WPA Pessoal* , e o Protocolo de Integridade de Chave Temporal (TKIP, pronunciado *tee-kip* ) para criptografia. *O WPA Enterprise* usa um servidor de autenticação para gerar chaves ou certificados.
- **Wi-Fi Protected Access version 2 (WPA2):**baseado no padrão de segurança sem fio 802.11i, que foi finalizado em 2004. O aprimoramento mais significativo do WPA2 sobre WPA é o uso do AES (Advanced Encryption Standard) para criptografia. A segurança fornecida pela AES é suficiente (e aprovada) para ser usada pelo governo dos EUA para criptografar informações classificadas como extremamente secretas

https://www.dummies.com/computers/computer-networking/wireless/wireless-security-protocols-wep-wpa-and-wpa2/

# CONTINUIDADE DE NEGÓCIO


- Inundação, Ataque cibernético, Falha na cadeia de suprimentos ou perda de um funcionário importante, Interrupções nos seus negócios podem ocorrer a qualquer momento.
- A continuidade dos negócios consiste em ter um plano para lidar com situações difíceis, para que sua organização possa continuar funcionando com o mínimo de interrupções possível.
- Seja uma empresa, organização do setor público ou instituição de caridade, você precisa saber como continuar em qualquer circunstância.
- Um bom plano de BC reconhece possíveis ameaças a uma organização e analisa qual o impacto que elas podem ter nas operações diárias.
- Ele também fornece uma maneira de atenuar essas ameaças, criando uma estrutura que permite que as principais funções da empresa continuem, mesmo que o pior aconteça.

https://www.thebci.org/knowledge/introduction-to-business-continuity.html

# BACKUPS

- Um **backup** é uma cópia dos dados importantes que são armazenados em um local alternativo, para que possam ser recuperados se excluídos ou corrompidos . Dependendo da frequência com que os dados são alterados, da importância e do tempo necessário para o backup, determina com que frequência o backup é feito.
- Por exemplo, uma empresa com registros de clientes que mudam frequentemente pode fazer backup de seus dados a cada poucas horas. Dados ainda mais confidenciais, como registros bancários, podem ser armazenados em unidades RAID que ajudam a proteger os dados, mesmo que a unidade falhe.
- Hoje, existem várias maneiras de fazer backup de suas informações e mídias para manter seus dados. Por exemplo, CD-R , DVD-R , drives USB , discos externos , e na nuvem são alguns dos lugares mais populares para backup de seus dados.

https://searchdatabackup.techtarget.com/definition/backup

# BACKUPS - TIPOS

**Backup completo**

- Como o nome sugere, isso se refere ao processo de copiar tudo o que é considerado importante e que não deve ser perdido. Esse tipo de backup é a primeira cópia e geralmente a cópia mais confiável, pois normalmente pode ser feita sem a necessidade de ferramentas adicionais.

**Backup incremental**

- Esse processo exige muito mais cuidado nas diferentes fases do backup, pois envolve a cópia dos arquivos, levando em consideração as alterações feitas neles desde o backup anterior. Por exemplo, imagine que você fez um backup completo. Quando terminar, você decide que, daqui para frente, fará backups incrementais e, em seguida, criará dois novos arquivos. O backup incremental detectará que todos os arquivos no backup completo permanecem os mesmos e fará apenas cópias de backup dos dois arquivos criados recentemente. Dessa forma, o backup incremental economiza tempo e espaço, pois sempre haverá menos arquivos para backup do que se você fizesse um backup completo. Recomendamos que você não tente empregar esse tipo de estratégia de backup usando meios manuais.

**Backup diferencial**

- Um backup diferencial tem a mesma estrutura básica que um backup incremental - em outras palavras, envolve fazer cópias apenas de novos arquivos ou de arquivos que sofreram algum tipo de alteração. No entanto, com esse modelo de backup, todos os arquivos criados desde o backup completo original sempre serão copiados novamente. Pelas mesmas razões que os backups incrementais, recomendamos que os backups diferenciais também não sejam executados manualmente.

https://www.welivesecurity.com/2019/05/10/types-backup-mistakes-avoid/

# CLOUDS BACKUP

- A nuvem (também conhecida como "computação em nuvem") refere-se à entrega sob demanda de recursos e serviços de computação pela Internet, com o pagamento conforme o uso.Essencialmente, a “nuvem” representa um pool compartilhado de vários recursos e serviços usados para armazenar, gerenciar e processar dados que podem ser acessados via web.A computação em nuvem permite eliminar os custos desnecessários associados à construção e manutenção da infraestrutura de TI local.

**O que é armazenamento em nuvem?**

- O armazenamento em nuvem é um modelo de armazenamento de dados no qual os dados podem ser acessados, gerenciados e armazenados em um servidor de nuvem remoto via Internet.O armazenamento em nuvem é mantido e suportado por um provedor de armazenamento em nuvem responsável por manter os dados do usuário disponíveis e acessíveis a qualquer momento.
- Geralmente, os sistemas de armazenamento em nuvem compartilham as seguintes características:
- 1. O provedor de armazenamento em nuvem é totalmente responsável pelo suporte e manutenção de back-end do aplicativo.
- 2. Os ambientes em nuvem funcionam com base no autoatendimento, o que significa que o usuário pode obter acesso direto aos recursos baseados na nuvem e usufruir dos serviços internos sem envolver o provedor de serviços.
- 3. Os ambientes em nuvem são elásticos.Assim, eles podem ser redimensionados para cima ou para baixo, dependendo das necessidades do cliente.
- 4. Os recursos baseados em nuvem podem ser acessados pela Internet a qualquer momento.
- 5. Um ambiente de nuvem pode ser compartilhado por vários usuários com a ajuda de um modelo de multilocatário.
- 6. O provedor de armazenamento em nuvem monitora e calcula o uso de recursos de cada usuário, o que significa que você paga apenas pelo que usa em um determinado período de tempo.

# CLOUD BACKUP - TIPOS

- Os seguintes tipos de armazenamento em nuvem podem ser diferenciados.

1. **O armazenamento em nuvem pública:** é essencialmente um ambiente de armazenamento com vários locatários usado principalmente para armazenar dados não estruturados e menos confidenciais.O armazenamento em nuvem pública funciona como um data center global, onde os recursos de computação podem ser armazenados e acessados pelo público em geral pela Internet.Os principais fornecedores de armazenamento em nuvem pública incluem Amazon Web Services (AWS), Microsoft Azure, plataforma Google Cloud, etc.
2. **O armazenamento em nuvem privada:** é um ambiente em nuvem usado por uma organização exclusivamente e geralmente gerenciado por recursos internos ou por um fornecedor de terceiros.As nuvens privadas são projetadas para organizações que exigem controle total de dados, personalização e segurança de alto nível.Os principais fornecedores de armazenamento em nuvem privada são VMware, Dell EMC, Hewlett Packard Enterprise (HPE), OpenStack etc.
3. **O armazenamento em nuvem híbrida:** representa uma combinação de armazenamento em nuvem pública e privada para formar um sistema abrangente.Nesse caso, dados críticos são armazenados na nuvem privada, enquanto dados menos sensíveis são transferidos para o armazenamento em nuvem pública.Para obter a máxima eficiência em um ambiente virtual, são utilizados os serviços de provedores de nuvem pública e privada.

https://www.nakivo.com/blog/introduction-cloud-backup/

# CLOUD BACKUP – IAAS, PAAS, SAAS

**IaaS — Infrastructure as a Service (Infraestrutura como Serviço)**

- Nesse primeiro exemplo dos modelos de nuvem, a empresa contrata uma capacidade de hardware que corresponde a memória, armazenamento, processamento etc. Podem entrar nesse pacote de contratações os servidores, roteadores, racks, entre outros.
- Dependendo do fornecedor e do modelo escolhido, a sua empresa pode ser tarifada, por exemplo, pelo número de servidores utilizados e pela quantidade de dados armazenados ou trafegados. Em geral, tudo é fornecido por meio de um data center com servidores virtuais, em que você paga somente por aquilo que usar.

**PaaS — Platform as a Service (Plataforma como Serviço)**

- Imagine que você contratou uma ótima solução para a sua empresa — que funciona na nuvem —, mas que não possui um recurso personalizado essencial para o seu trabalho.
- Nesse cenário, o PaaS surge como o ideal porque é, como o próprio nome diz, uma plataforma que pode criar, hospedar e gerir esse aplicativo.
- Nesse modelo de nuvem, contrata-se um ambiente completo de desenvolvimento, no qual é possível criar, modificar e otimizar softwares e aplicações.
- Tudo isso é feito utilizando a infraestrutura na nuvem. Ou seja, o time de desenvolvimento tem uma infraestrutura completa e moderna à disposição, sem que sejam necessários altos investimentos.

# CLOUD BACKUP – IAAS, PAAS, SAAS

**SaaS — Software as a Service (Software como Serviço)**

- Por fim, qualquer pessoa conhece o SaaS, mesmo que não saiba. Nesse terceiro modelo de nuvem, você pode ter acesso ao software sem comprar a sua licença, utilizando-o a partir da Cloud Computing, muitas vezes com recursos limitados.
- No entanto, também existem planos de pagamento nos quais é cobrada uma taxa fixa ou um valor que varia de acordo com o uso. Muitos CRMs ou ERPs trabalham no sistema SaaS.
- Assim, o acesso a esses softwares é feito usando a internet. Os dados, contatos e demais informações podem ser acessados de qualquer dispositivo, dando mais mobilidade à equipe.
- Falamos que qualquer um conhece o SaaS porque sites como o Facebook e o Twitter ou aplicativos como o Skype, OneDrive, Google Docs e o Office 365 funcionam dessa maneira.
- Neles, tudo é disponibilizado na nuvem, para que muitos usuários consigam ter acesso ao serviço pelo browser ou por um software — como no caso do Skype.

https://brasil.softlinegroup.com/sobre-a-empresa/blog/iaas-paas-saas-nuvem

# SECURITY OPERATION CENTER

- Um centro de operações de segurança ( **SOC** ) é uma instalação que abriga uma equipe de segurança da informação responsável por monitorar e analisar continuamente a postura de segurança de uma organização. O objetivo da equipe do SOC é detectar, analisar e responder a incidentes de segurança cibernética usando uma combinação de soluções de tecnologia e um forte conjunto de processos. Os centros de operações de segurança normalmente contam com analistas e engenheiros de segurança, além de gerentes que supervisionam as operações de segurança. A equipe do SOC trabalha em conjunto com as equipes organizacionais de **resposta a incidentes** para garantir que os problemas de segurança sejam resolvidos rapidamente após a descoberta.
- Os centros de operações de segurança monitoram e analisam a atividade em redes, servidores, terminais, bancos de dados, aplicativos, sites e outros sistemas, procurando atividades anômalas que possam ser indicativas de um incidente ou comprometimento da segurança. O SOC é responsável por garantir que possíveis incidentes de segurança sejam corretamente identificados, analisados, defendidos, investigados e relatados.

# SECURITY OPERATION CENTER – COMO FUNCIONA

- Em vez de focar no desenvolvimento de estratégia de segurança, projetar arquitetura de segurança ou implementar medidas de proteção, a equipe do SOC é responsável pelo componente operacional contínuo da segurança da informação corporativa. A equipe do centro de operações de segurança é composta principalmente por analistas de segurança que trabalham juntos para detectar, analisar, responder, relatar e prevenir incidentes de segurança cibernética. Recursos adicionais de alguns SOCs podem incluir análise forense avançada, análise de criptografia e engenharia reversa de malware para analisar incidentes.
- O primeiro passo para estabelecer o SOC de uma organização é definir claramente uma **estratégia** que incorpore objetivos específicos de negócios de vários departamentos, bem como informações e suporte de executivos. Uma vez desenvolvida a estratégia, a infraestrutura necessária para dar suporte a essa estratégia deve ser implementada. De acordo com Pierluigi Paganini, diretor de segurança da informação do Bit4Id, **infraestrutura** típica de SOCinclui firewalls, IPS / IDS, soluções de detecção de violação, probes e um sistema de gerenciamento de informações e eventos de segurança (SIEM). A tecnologia deve estar em vigor para coletar dados por meio de fluxos de dados, telemetria, captura de pacotes, syslog e outros métodos, para que a atividade dos dados possa ser correlacionada e analisada pela equipe do SOC. O centro de operações de segurança também monitora redes e pontos de extremidade quanto a vulnerabilidades, a fim de proteger dados confidenciais e cumprir as regulamentações do setor ou do governo.

# RESPOSTA A INCIDENTES

- Resposta a incidentes é a metodologia que uma organização usa para responder e gerenciar um ataque cibernético. Um ataque ou violação de dados pode causar estragos potencialmente afetando clientes, tempo e recursos da empresa de propriedade intelectual e valor da marca. Uma resposta a incidentes visa reduzir esse dano e recuperar o mais rápido possível. A investigação também é um componente essencial para aprender com o ataque e se preparar melhor para o futuro. Como muitas empresas hoje enfrentam uma violação em algum momento, um plano de resposta a incidentes bem desenvolvido e repetível é a melhor maneira de proteger sua empresa.
- **Preparação:** Desenvolvimento de políticas e procedimentos a serem seguidos em caso de violação cibernética. Isso incluirá determinar a composição exata da equipe de resposta e os gatilhos para alertar os parceiros internos. A chave desse processo é o treinamento eficaz para responder a uma violação e documentação para registrar as ações tomadas para análise posterior.
- **Identificação:** este é o processo de detectar uma violação e permitir uma resposta rápida e focada. As equipes de segurança de TI identificam violações usando vários fluxos de inteligência de ameaças, sistemas de detecção de intrusões e firewalls. Algumas pessoas não entendem o que é inteligência de ameaças, mas é fundamental para proteger sua empresa. Os profissionais de inteligência de ameaças analisam as tendências atuais de ameaças cibernéticas, táticas comuns usadas por grupos específicos e mantêm sua empresa um passo à frente.
- **Contenção:** Uma das primeiras etapas após a identificação é conter os danos e impedir uma maior penetração. Isso pode ser feito colocando sub-redes específicas offline e confiando nos backups do sistema para manter as operações. Sua empresa provavelmente permanecerá em estado de emergência até que a violação seja contida.

# RESPOSTA A INCIDENTES

- **Erradicação:** Este estágio envolve neutralizar a ameaça e restaurar os sistemas internos o mais próximo possível do estado anterior. Isso pode envolver monitoramento secundário para garantir que os sistemas afetados não estejam mais vulneráveis a ataques subseqüentes.
- **Recuperação:** as equipes de segurança precisam validar se todos os sistemas afetados não estão mais comprometidos e podem retornar à condição de trabalho. Isso também requer a definição de cronogramas para restaurar totalmente as operações e o monitoramento contínuo de qualquer atividade anormal da rede. Nesse estágio, torna-se possível calcular o custo da violação e os danos subsequentes.
- **Lições aprendidas:** Um dos estágios mais importantes e muitas vezes esquecidos. Durante esse estágio, a equipe de resposta a incidentes e os parceiros se reúnem para determinar como melhorar os esforços futuros. Isso pode envolver a avaliação de políticas e procedimentos atuais, bem como decisões específicas que a equipe tomou durante o incidente. A análise final deve ser condensada em um relatório e usada para treinamento futuro. O Forcepoint pode ajudar sua equipe a analisar incidentes anteriores e melhorar seus procedimentos de resposta. Proteger sua organização requer um esforço determinado para aprender e fortalecer constantemente sua rede contra agentes maliciosos.

# LOG MONITOR E LOG ANALYZER

- **O monitoramento de logs** é o ato de revisar os logs coletados à medida que são registrados. Isso normalmente envolve a assistência do software de gerenciamento de log. O software de gerenciamento de logs pode ser configurado para escutar eventos específicos do aplicativo e alertar as pessoas apropriadas em uma organização de desenvolvimento quando esse evento ocorrer, entre outros benefícios.
  **Análise de log**, por outro lado, é um processo normalmente executado por desenvolvedores ou outras pessoas de TI dentro de uma organização por vários motivos - geralmente relacionados à solução de problemas em um sistema ou aplicativo. Os logs coletados são usados para diagnosticar e resolver problemas em um aplicativo.
  Esse é o resumo geral da diferença entre análise de log e monitoramento de log, mas vamos aprofundar.

**SIEM**

- O software de gerenciamento de informações e eventos de segurança (SIEM) oferece aos profissionais de segurança uma visão e um histórico das atividades em seu ambiente de TI.
- A tecnologia SIEM existe há mais de uma década, inicialmente evoluindo a partir da disciplina de gerenciamento de logs. Ele combinou o gerenciamento de eventos de segurança (SEM) – que analisa dados de log e eventos em tempo real para fornecer monitoramento de ameaças, correlação de eventos e resposta a incidentes – com gerenciamento de informações de segurança (SIM) que coleta, analisa e gera relatórios.

# LOG MONITOR E LOG ANALYZER

- O software SIEM coleta e agrega dados de log gerados em toda a infraestrutura de tecnologia da organização, desde sistemas host e aplicativos até dispositivos de rede e segurança, como firewalls e filtros antivírus.
- O software identifica e categoriza incidentes e eventos, além de analisá-los. O software oferece dois objetivos principais, que são: fornecer relatórios sobre incidentes e eventos relacionados à segurança, como logins bem-sucedidos e com falha, atividade de malware e outras possíveis atividades mal-intencionadas e enviar alertas se a análise mostrar que uma atividade é executada em conjuntos de regras predeterminados e, portanto, indica um possível problema de segurança.

# ANTIVÍRUS

- O software antivírus é um programa ou conjunto de programas projetados para impedir, pesquisar, detectar e remover vírus de software e outro software malicioso, como worms, cavalos de Troia, adware e muito mais.
- Essas ferramentas são essenciais para que os usuários estejam instalados e atualizados, pois um computador sem proteção de software antivírus será infectado em poucos minutos após a conexão com a Internet. O bombardeio é constante, o que significa que as empresas de antivírus precisam atualizar suas ferramentas de detecção regularmente para lidar com os mais de 60.000 novos tipos de malware criados diariamente.
- O malware de hoje (um termo abrangente que engloba vírus de computador) muda a aparência rapidamente para evitar a detecção por software antivírus mais antigo, baseado em definições. Os vírus podem ser programados para causar danos ao seu dispositivo, impedir que um usuário acesse dados ou para controlar o seu computador.
- Várias empresas diferentes criam software antivírus e cada oferta pode variar, mas todas desempenham algumas funções essenciais:

- Examine arquivos ou diretórios específicos em busca de malware ou padrões maliciosos conhecidos
- Permite agendar verificações para executar automaticamente para você
- Permite iniciar uma verificação de um arquivo específico ou de todo o computador ou de um CD ou unidade flash a qualquer momento.
- Remova qualquer código malicioso detectado - às vezes você será notificado sobre uma infecção e perguntado se deseja limpar o arquivo, outros programas farão isso automaticamente nos bastidores.
- Mostrar a "saúde" do seu computador

# ENDPOINT PROTECTION

- O **Endpoint Protection** é uma suite de proteção para laptops, desktops e servidores (“endpoints”) em rede contra vírus, worms, cavalos de tróia, spywares, adwares, rootkits e ameaças desconhecidas (“ataques dia zero”). Para proteção desses ataques avançados o endpoint combina várias tecnologias uma única interface:
- Antivírus e anti-spyware: verificação para vírus e riscos de segurança
- Firewall pessoal: evita que usuários sem autorização acessem os computadores e as redes se conectam à rede
- Prevenção de intrusão: age como a segunda camada de defesa do cliente depois do firewall
- Verificação protetiva de ameaças: analisa o comportamento de um aplicativo para determinar se ele tem as características de ameaças
- Controle de dispositivos: bloqueia ou permite o acesso de dispositivos, tais como portas USB, infravermelhos, portas seriais e paralelas.
- Controle de aplicativos: bloqueia e permite aplicativos que tentem acessar os recursos do sistema

# WIRESHARK

- O Wireshark é um programa que analisa o tráfego de rede, e o organiza por protocolos. As funcionalidades do Wireshark são parecidas com o tcpdump mas com uma interface gráfica, com mais informação e com a possibilidade da utilização de filtros.
- Eu recomendo para você aprender redes e entender como ela trabalha e suas formas de comunicação.
- https://www.comparitech.com/net-admin/wireshark-cheat-sheet/
- https://medium.com/hacker-toolbelt/wireshark-filters-cheat-sheet-eacdc438969c
- https://packetlife.net/blog/2008/oct/18/cheat-sheets-tcpdump-and-wireshark/

# AONDE APRENDER MAIS?

- Enfim, esse são alguns conceitos de segurança de redes, claro que minha recomendação é que você pesquise e se aprofunde cada vez mais, principalmente conhecer as principais soluções do mercado, à minha recomendação é procurar por gartners de soluções em vários aspectos, seja um Analise e Monitoramento de Redes, Analise de Vulnerabilidades, Firewalls, Antivírus, IDS e IPS e etc;
- A minha recomendação é que você procure técnicas e métodos para implementar segurança na sua empresa, pois segurança de redes vai além de apenas proteger uma rede de comunicação, mas sim pessoas também;
- Cada conteúdo apresentado foi tirado das certificações **CND (Certified Network Defender) da EC-COUNCIL (**https://acaditi.com.br/cnd-treinamento-certified-network-defender/), **do Network Security Fundamentals da EC-COUNCIL** (https://acaditi.com.br/nsf-treinamento-network-security-fundamentals/), além dos conteúdos relacionados a **CCNA CISCO** (https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/associate/ccna-security.html), **Network+ CompTIA** (https://www.comptia.org/pt/certificacoes/network) **e Security+ CompTIA** (https://www.comptia.org/pt/certificacoes/security)
- Além disso, recomendo livros relacionados a segurança da informação e segurança de redes;
- Por fim, caso queira materiais extras ou outros detalhes, eu tenho diversos artigos no LinkedIn sobre o assunto:

https://www.linkedin.com/in/joas-antonio-dos-santos/

# CONCLUSÃO

- Esses foram alguns conteúdos básicos que eu tinha para apresentar, caso você deseja se aprofundar mais ainda é essencial aprender fundamentos antes obviamente, principalmente fundamentos de redes, segurança da informação e base computacional;
- Por recomendação, desenvolva laboratórios  para aprimorar suas habilidades também,  caso queira alguma base, veja meu Challenges sobre SOC https://bit.ly/3izyRS3
- Por fim, não se prenda apenas à soluções, tendo a base com certeza você vai conseguir trabalhar com qualquer uma. E claro, não apresentei nem 10% do conteúdo real que envolve segurança de redes e afins, mas existem muitos conteúdos na internet e até mesmo como na página anterior, tem diversas certificações.

**Alguns materiais:**

- https://github.com/fabionoth/awesome-cyber-security
- https://github.com/sbilly/awesome-security
- https://github.com/emtuls/Awesome-Cyber-Security-List
- https://github.com/onlurking/awesome-infosec

Desde já, agradeço por ler até aqui

# OBRIGADO!

# REFERENCE


https://alcidesmaya.edu.br/redes-de-computadores/o-que-sao-redes-de-computadores/
https://www.belden.com/blog/smart-building/network-types
https://www.iperiusbackup.net/pt-br/entendendo-os-conceitos-entre-os-modelos-tcpip-e-osi/
https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/
https://www.javatpoint.com/computer-network-tcp-ip-model
https://www.geeksforgeeks.org/tcp-ip-model/?ref=lbp
https://www.guru99.com/tcp-ip-model.html
https://www.cloudflare.com/learning/network-layer/internet-protocol/
https://www.geeksforgeeks.org/differences-between-ipv4-and-ipv6/
https://pplware.sapo.pt/tutoriais/redes-quais-diferencas-protocolo-tcp-udp/
https://pt.wikipedia.org/wiki/M%C3%A1scara_de_rede
https://www.interserver.net/tips/kb/common-network-protocols-ports/
https://searchnetworking.techtarget.com/definition/TCP-IP
https://pt.wikipedia.org/wiki/Lista_de_portas_dos_protocolos_TCP_e_UDP
https://www.gta.ufrj.br/grad/99_1/fernando/roteamento/protoc1.htm#:~:text=Roteamento%20%C3%A9%20o%20processo%20pelo,EGP%20(Exterior%20Gateway%20Protocol).
https://www.gta.ufrj.br/grad/02_2/ospf/ospf.html#:~:text=OSPF%20%C3%A9%20um%20protocolo%20de,(Internet%20Engineering%20Task%20Force).
http://paginas.unisul.br/carlos.luz/redes/ROTEAMENTO_DINAMICO/VLSR_CIRD.pdf

# REFERENCE


https://pplware.sapo.pt/tutoriais/networking/redes-saiba-o-que-e-uma-vlan-e-aprenda-a-configurar/
https://www.gta.ufrj.br/grad/02_2/vlans/definicao.html
http://www.dltec.com.br/blog/redes/o-que-e-vlan/
https://brainwork.com.br/2012/08/12/vtp-stp-e-a-mudana-de-paradigma/
https://www.cisco.com/c/pt_br/support/docs/lan-switching/vtp/10558-21.html
https://cartilha.cert.br/redes/
https://blog.knowbe4.com/great-defense-in-depth-infographic
http://www.sp.senac.br/normasadministrativas/psi_normas_administrativas.pdf
https://www.csoonline.com/article/3263738/9-policies-and-procedures-you-need-to-know-about-if-youre-starting-a-new-security-program.html
https://www.bmc.com/blogs/security-vulnerability-vs-threat-vs-risk-whats-difference/
http://www.uobabylon.edu.iq/eprints/publication_3_25852_324.pdf
https://www.baboo.com.br/artigos/como-antivirus-funcionam/
https://www.youtube.com/watch?v=ps9ntazo1v0
https://www.welivesecurity.com/2015/03/31/6-ways-to-back-up-your-data/
https://www.techopedia.com/definition/31435/password-manager
https://searchcompliance.techtarget.com/definition/risk-management
https://www.geeksforgeeks.org/cryptography-and-its-types/