**Introdução**

21.0.1

**Por que devo fazer este módulo?**

O que você sabe sobre criptografia? O que é e como pode ser implementado? Para proteger os dados à medida que eles viajam através de links, você precisa ter um entendimento de como proteger esses dados e manter sua integridade. Neste módulo você vai aprender sobre criptografia e seu papel na comunicação de dados digitais. Vamos começar!

21.0.2

**O que vou aprender neste módulo?**

**Título do módulo:** criptografia de chave pública

**Objetivo do módulo:** Explicar como a infraestrutura de chave pública (PKI) oferece suporte à segurança de rede.

| **Título do Tópico** | **Objetivo do Tópico** |
| --- | --- |
| Integridade e Autenticidade | Explique a função da criptografia para garantir a integridade e autenticidade dos dados. |
| Confidencialidade | Explicar como as abordagens criptográficas aumentam a confidencialidade dos dados. |
| Criptografia de chave pública | Explicar a criptografia de chave pública. |
| Autoridades e o Sistema de Confiança PKI | Explicar como funciona a infraestrutura de chave pública. |
| Aplicações e impactos da criptografia | Explicar como o uso da criptografia afeta as operações de segurança cibernética. |

# Integridade e Autenticidade

21.1.1

## Comunicações seguras

As organizações devem fornecer suporte para proteger os dados à medida que eles viajam pelos links. Isso pode incluir tráfego interno, mas é mais importante proteger os dados que viajam para fora da organização para as filiais, locais de trabalho remoto, e parceiros.

Estes são os quatro elementos das comunicações seguras:

* **Integridade dos dados** - Garante que a mensagem não foi alterada. Quaisquer alterações nos dados em trânsito serão detectadas. A integridade é garantida pela implementação de um dos algoritmos Secure Hash (SHA-2 ou SHA-3). O algoritmo de resumo de mensagens MD5 ainda está amplamente em uso, no entanto, é inerentemente inseguro e cria vulnerabilidades em uma rede. O uso de MD5 deve ser evitado.
* **Autenticação da origem** - Garante que a mensagem não é uma falsificação e realmente vem de quem afirma. Muitas redes modernas garantem autenticação com algoritmos como código de autenticação de mensagem baseado em hash (HMAC).
* **Confidencialidade dos dados**- Garante que apenas usuários autorizados possam ler a mensagem. Se a mensagem for interceptada, ela não poderá ser decifrada dentro de um razoável período de tempo. A confidencialidade dos dados é implementada usando algoritmos de criptografia simétrica e assimétrica.
* **Dados não repudiáveis** - Garante que o remetente não possa repudiar ou refutar a validade de uma mensagem enviada. O não repúdio depende do fato de que apenas o remetente possui as características ou a assinatura exclusivas de como essa mensagem é tratada.

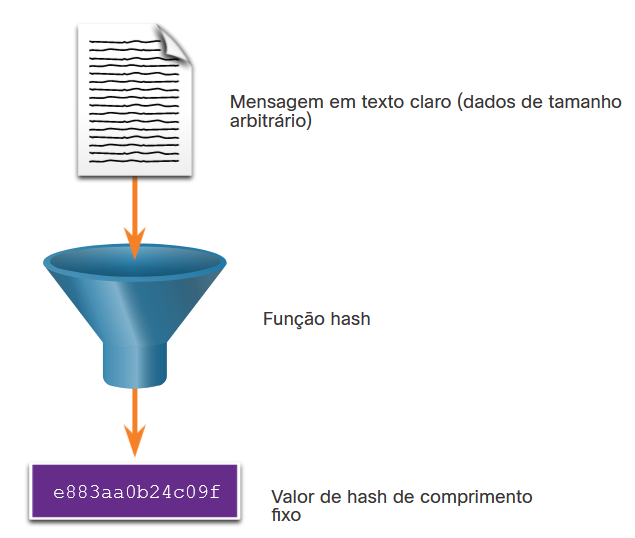
A criptografia pode ser usada em praticamente qualquer lugar em que haja comunicação de dados. De fato, a tendência é que toda comunicação seja criptografada.

21.1.2

## Funções criptográficas de hash

Hashes são usados para verificar e garantir a integridade dos dados. O hash é baseado em uma função matemática unilateral que é relativamente fácil de calcular, mas significativamente mais difícil de reverter. A moagem de café é uma boa analogia de função unidirecional. É fácil moer grãos de café, mas é quase impossível unir novamente todos os pedaços para reconstruir os grãos originais. A função de hash criptográfico também pode ser usada para verificar a autenticação.

A figura mostra um pedaço de papel impresso com palavras para o lado: mensagem de texto simples (dados de comprimento arbitrário). Uma seta vai do papel para um funil que tem a função hash palavras ao lado dele. Uma seta sai do funil para uma caixa de texto: e883aacb24c09f e as palavras valor de hash de comprimento fixo.



Como mostrado na figura, uma função hash leva um bloco variável de dados binários, chamado de mensagem, e produz uma representação condensada de comprimento fixo, chamado hash. O hash resultante também é às vezes chamado de mensagem digest, digest ou impressão digital.

Com funções hash, é computacionalmente inviável que dois conjuntos diferentes de dados apresentem a mesma saída hash. Cada vez que os dados são modificados ou alterados, o valor de hash também muda. Por isso, muitas vezes os valores criptográficos de hash são chamados de impressões digitais. Eles podem ser usados para detectar arquivos de dados duplicados, alterações de versão de arquivo e aplicativos semelhantes. Esses valores são usados para proteger contra uma alteração acidental ou intencional dos dados ou corrupção acidental dos dados.

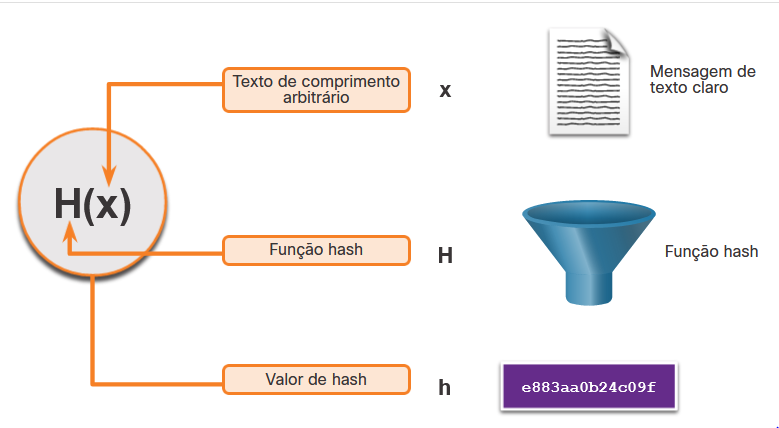
A função hash criptográfico é aplicada em muitas situações diferentes para autenticação de entidade, integridade de dados e fins de autenticidade de dados.

21.1.3

## Operação de hash criptográfico

Matematicamente, a equação **h= H(x)** é usada para explicar como um algoritmo de hash opera. Como mostrado na figura, uma função hash H leva uma entrada x e retorna um valor hash string de tamanho fixo h.

A figura mostra um círculo com H(x) dentro do círculo. Na parte superior há uma caixa de texto que diz texto de comprimento arbitrário e uma seta indo para o círculo apontando para o x. À direita da caixa de texto está x e um ícone para uma mensagem de texto simples. No centro é uma caixa de texto com a função hash palavras e uma seta apontando para o h dentro do círculo. Há um H à direita da caixa de texto, um ícone de funil e a função de hash palavras. Na parte inferior está uma caixa de texto que leva a partir do círculo e tem as palavras valor hash, a letra h ao lado da caixa de texto e um retângulo que tem e883aa0b24c09f nele.



O exemplo na figura resume o processo matemático. Uma função hash criptográfica deve ter as seguintes propriedades:

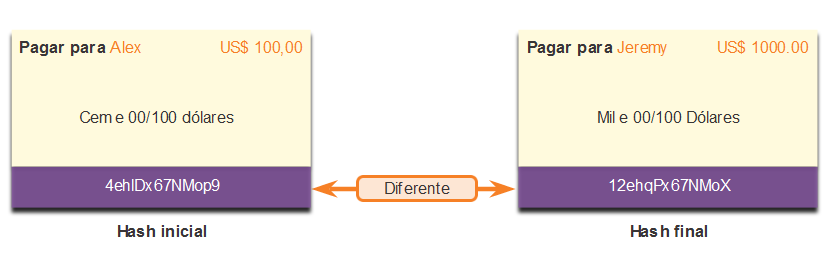
* A entrada pode ser de qualquer comprimento.
* A saída tem um comprimento fixo.
* H(x) é relativamente fácil de calcular para qualquer x.
* H(x) é um caminho e não reversível.
* H(x) é livre de colisões, o que significa que dois valores de entrada diferentes resultarão em valores de hash diferentes.

Se uma função hash é difícil de inverter, ela é considerada um hash unidirecional. Difícil de inverter significa que dado um valor de hash de h, é computacionalmente inviável encontrar uma entrada para x tal que h=h (x).

21.1.4

## MD5 e SHA

As funções de hash são usadas para garantir a integridade de uma mensagem. Eles garantem que os dados não foram alterados acidentalmente ou intencionalmente. Na figura, o remetente está enviando uma transferência de dinheiro de US $ 100 para Alex. O remetente deseja garantir que a mensagem não seja alterada acidentalmente no caminho para o destinatário. Alterações deliberadas que são feitas por um ator ameaça ainda são possíveis.



A figura mostra os cálculos de hash de uma mensagem na qual o hash inicial e o final são diferentes. A mensagem enviada diz: Pague a Alex $ 100,00. A mensagem recebida diz: Pague a Jeremy $ 1000,00. O hash inicial é 4ehiDx67NMop9 e o final é 12ehqPx67NMoX.

**Pagar para** AlexUS$ 100,00Cem e 00/100 dólares4ehlDx67NMop9Hash inicial**Pagar para** JeremyUS$ 1000.00Mil e 00/100 Dólares12ehqPx67NMoXHash finalDiferente

O algoritmo de hash funciona da seguinte forma:

1. O dispositivo de envio insere a mensagem em um algoritmo de hashing e calcula seu hash de comprimento fixo de **4ehiDx67NMop9**.
2. Esse hash é anexado à mensagem e enviado ao destinatário. A mensagem e o hash estão em texto sem formatação.
3. O dispositivo receptor remove o hash da mensagem e insere a mensagem no mesmo algoritmo de hash. Se o hash calculado for igual ao que está anexado à mensagem, a mensagem não foi alterada durante o trânsito. Se os hashes não forem iguais, conforme mostrado na figura, a integridade da mensagem não será mais confiável.

Existem quatro funções hash bem conhecidas:

* **MD5 com resumo de 128 bits** - Desenvolvido por Ron Rivest e usado em uma variedade de aplicações de internet, MD5 é uma função unidirecional que produz uma mensagem hash de 128 bits. MD5 é considerado um algoritmo legado e deve ser evitado e usado apenas quando não houver alternativas melhores disponíveis. Recomenda- se que SHA-2 ou SHA-3 sejam usados em vez disso.
* **SHA-1** — Desenvolvido pela Agência de Segurança Nacional dos EUA (NSA) em 1995. É muito semelhante às funções hash MD5. Existem várias versões. O SHA-1 cria uma mensagem de 160 bits e é um pouco mais lento que o MD5. O SHA-1 possui falhas conhecidas e é um algoritmo antigo.
* **SHA-2** — Desenvolvido pela NSA. Inclui SHA-224 (224 bits), SHA-256 (256 bits), SHA-384 (384 bits) e SHA-512 (512 bits). Se você estiver usando SHA-2, então os algoritmos SHA-256, SHA-384 e SHA-512 devem ser usados sempre que possível.
* **SHA-3** - SHA-3 é o mais novo algoritmo de hash e foi introduzido pelo NIST como uma alternativa e eventual substituição para a família SHA-2 de algoritmos de hash. SHA-3 inclui SHA3-224 (224 bits), SHA3-256 (256 bits), SHA3-384 (384 bits) e SHA3-512 (512 bits). A família SHA-3 são algoritmos de última geração e devem ser usados sempre que possível.

Embora o hashing possa ser usado para detectar alterações acidentais, ele não pode ser usado para proteger contra alterações deliberadas feitas por um agente de ameaça. Não há informações de identificação única do remetente no procedimento de hash. Isso significa que qualquer pessoa pode processar um hash para quaisquer dados, desde que tenha a função hash correta.

Por exemplo, quando a mensagem atravessa a rede, um invasor em potencial pode interceptar a mensagem, alterá-la, recalcular o hash e anexá-lo à mensagem. O dispositivo receptor só validará contra o hash que estiver anexado.

Portanto, hash é vulnerável a ataques man in the middle e não oferece segurança aos dados transmitidos. Para fornecer autenticação de integridade e origem, é necessário algo mais.

**Observação: Os algoritmos** de hash protegem somente contra alterações acidentais e não protegem os dados contra alterações feitas deliberadamente por um ator de ameaça.

21.1.5

## autenticação da origem

Para adicionar autenticação de origem e garantia de integridade, use um código de autenticação de mensagem hash com chave (HMAC). HMACs usam uma chave secreta adicional como entrada à função hash.

**Observação:** Outros métodos MAC (Message Authentication Code) também são usados. No entanto, o HMAC é usado em muitos sistemas, incluindo SSL, IPsec e SSH.

**Algoritmo de Hash HMAC**

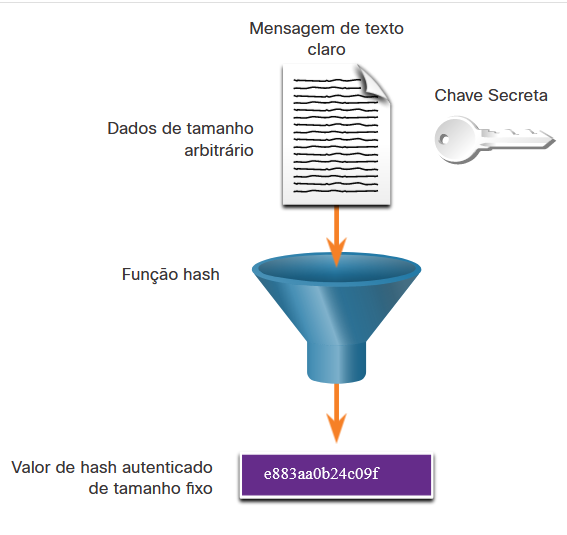
Conforme mostrado na figura, um HMAC é calculado usando qualquer algoritmo criptográfico que combina uma função hash criptográfica com uma chave secreta. As funções de hash são a base do mecanismo de proteção dos HMACs.

Somente o remetente e o destinatário têm conhecimento da chave secreta e agora a saída da função hash depende dos dados de entrada e da chave secreta. Apenas as partes que têm acesso a essa chave secreta podem calcular o digest de uma função HMAC. Isso derrota os ataques man-in-the-middle e fornece autenticação da origem dos dados.

Se duas partes compartilharem uma chave secreta e usarem as funções HMAC para autenticação, uma mensagem HMAC adequadamente construída, a parte recebeu indica que a outra parte foi a originadora da mensagem. Isso ocorre porque a outra parte possui a chave secreta.

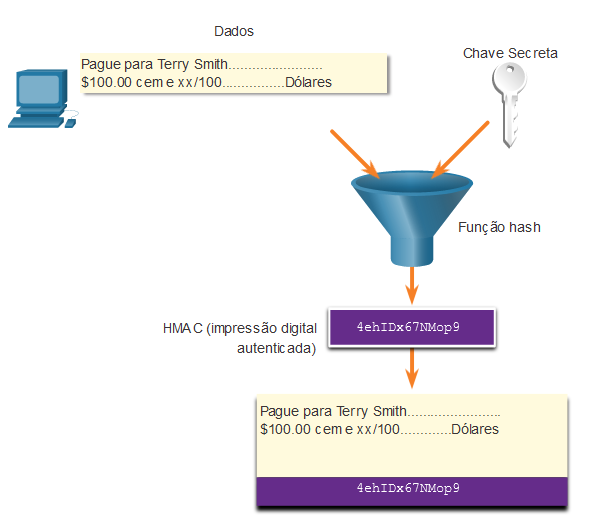
e883aa0b24c09f

Valor de hash autenticado de tamanho fixoDados de tamanho arbitrárioChave SecretaFunção hashMensagem de texto claro



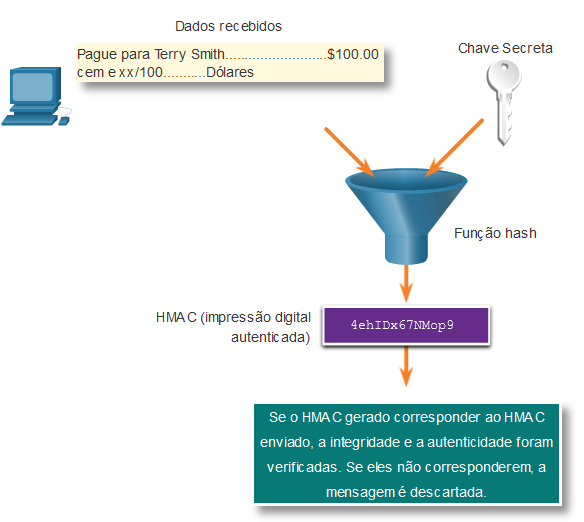
**Criação do valor de HMAC**

Conforme mostrado na figura, o dispositivo de envio insere dados (como o pagamento de Terry Smith de US $ 100 e a chave secreta) no algoritmo de hash e calcula o HMAC Digest de comprimento fixo. Esse Digest autenticado é anexado à mensagem e enviado ao destinatário.



**Verificação do valor de HMAC**

Na figura, o dispositivo receptor remove o Digest da mensagem e usa a mensagem de texto sem formatação com sua chave secreta como entrada na mesma função de hash. Se o Digest calculado pelo dispositivo receptor for igual ao resumo enviado, a mensagem não foi alterada. Adicionalmente, a origem da mensagem é autenticada porque apenas o remetente possui uma cópia da chave secreta compartilhada. A função HMAC garantiu a autenticidade da mensagem.

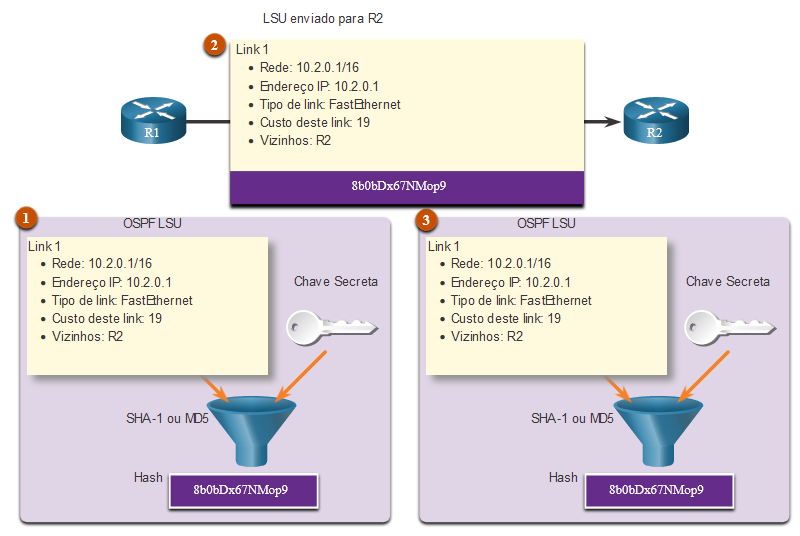


**Exemplo do Cisco Router HMAC**

A figura mostra como os HMACs são usados pelos roteadores Cisco configurados para usar a autenticação de roteamento Open Shortest Path First (OSPF).

R1 está enviando uma atualização de estado do link (LSU) referente a uma rota para a rede 10.2.0.0/16:

1. R1 calcula o valor do hash usando a mensagem LSU e a chave secreta.
2. O valor do hash resultante é enviado com o LSU para o R2.
3. R2 calcula o valor do hash usando o LSU e sua chave secreta. R2 aceita a atualização se os valores de hash corresponderem. Se eles não corresponderem, o R2 descartará a atualização.



# Confidencialidade

21.2.1

## Sigilo dos dados

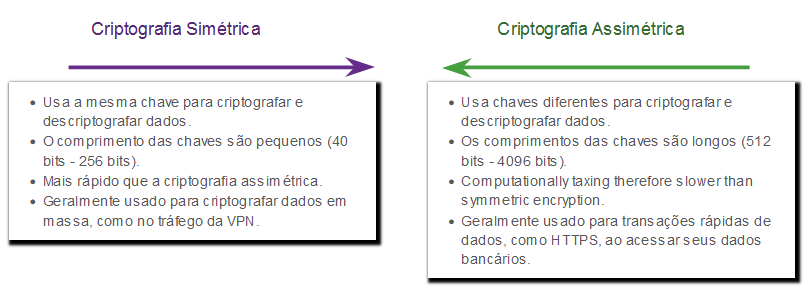
Existem duas classes de criptografia usadas para fornecer confidencialidade de dados; assimétrico e simétrico. Essas duas classes diferem na maneira como usam as chaves.

Algoritmos de criptografia simétrica, como Data Encryption Standard (DES), 3DES e Advanced Encryption Standard (AES), baseiam-se na premissa de que cada parte que se comunica conhece a chave pré-compartilhada. A confidencialidade dos dados também pode ser garantida usando algoritmos assimétricos, incluindo Rivest, Shamir e Adleman (RSA) e a infraestrutura de chave pública (PKI).

**Nota: O** DES é um algoritmo legado e não deve ser usado. 3DES deve ser evitado, se possível.

A figura destaca algumas diferenças entre criptografia simétrica e assimétrica.

A figura mostra as diferenças entre criptografia simétrica e assimétrica. As características da criptografia simétrica incluem: use a mesma chave para criptografar e descriptografar dados; os comprimentos das chaves são curtos (40 bits - 256 bits); mais rápido que a criptografia assimétrica; e geralmente usado para criptografar dados em massa, como no tráfego da VPN.



As características da criptografia assimétrica incluem: usa chaves diferentes para criptografar e descriptografar dados; os comprimentos das chaves são longos (512 bits - 4096 bits); muitas tarefas computacionalmente, portanto, mais lentas que a criptografia simétrica; e comumente usado para transações rápidas de dados, como HTTPS, ao acessar seus dados bancários.

Criptografia SimétricaCriptografia Assimétrica

* Usa a mesma chave para criptografar e descriptografar dados.
* O comprimento das chaves são pequenos (40 bits - 256 bits).
* Mais rápido que a criptografia assimétrica.
* Geralmente usado para criptografar dados em massa, como no tráfego da VPN.
* Usa chaves diferentes para criptografar e descriptografar dados.
* Os comprimentos das chaves são longos (512 bits - 4096 bits).
* Computationally taxing therefore slower than symmetric encryption.
* Geralmente usado para transações rápidas de dados, como HTTPS, ao acessar seus dados bancários.

21.2.2

## Criptografia Simétrica

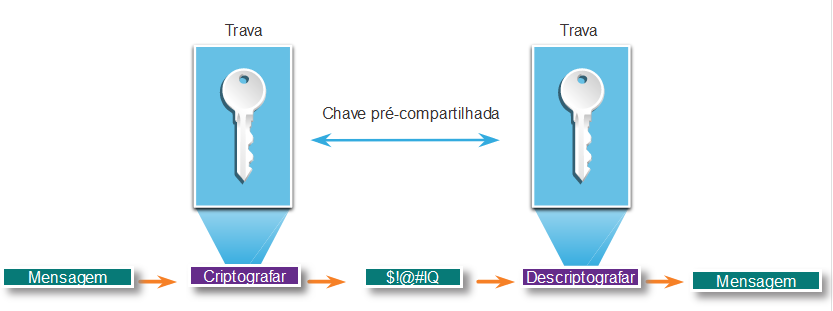
Os algoritmos simétricos usam a mesma chave pré-compartilhada para criptografar e descriptografar dados. Uma chave pré-compartilhada, também chamada de chave secreta, é conhecida pelo remetente e pelo receptor antes que qualquer comunicação criptografada possa ocorrer.

Para ajudar a ilustrar como a criptografia simétrica funciona, considere um exemplo em que Alice e Bob moram em locais diferentes e desejam trocar mensagens secretas entre si por meio do sistema de correio. Alice deseja enviar uma mensagem secreta para Bob.

Na figura, Alice e Bob têm chaves idênticas para um único cadeado. A troca de chaves aconteceu antes de enviar quaisquer mensagens secretas. Alice escreve uma mensagem secreta e a coloca em uma pequena caixa trancada com o cadeado. Ela manda a caixa para Bob. A mensagem está segura e trancada dentro da caixa, à medida que a caixa segue seu caminho através do sistema de correios. Quando Bob recebe a caixa, ele usa a chave para destrancar o cadeado e recuperar a mensagem. Bob pode usar a mesma caixa e cadeado para enviar uma resposta secreta para Alice.

A figura mostra a analogia de criptografia simétrica descrita no texto.

### Exemplo de criptografia simétrica



TravaTravaChave pré-compartilhada$!@#IQCriptografarMensagemDescriptografarMensagem

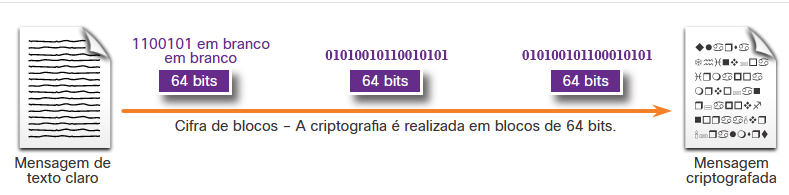
Hoje, algoritmos de criptografia simétrica são comumente usados com o tráfego VPN. Isso ocorre porque os algoritmos simétricos usam menos recursos da CPU do que os algoritmos de criptografia assimétrica. Isso permite que a criptografia e a descriptografia de dados sejam rápidas ao usar uma VPN. Ao usar algoritmos de criptografia simétrica, como qualquer outro tipo de criptografia, quanto maior a chave, mais tempo levará para alguém descobrir a chave. A maioria das chaves de criptografia tem entre 112 e 256 bits. Para garantir que a criptografia é segura, um comprimento mínimo de chave de 128 bits deve ser usado. Use uma chave mais longa para comunicações mais seguras.

Algoritmos de criptografia simétrica às vezes são classificados como uma cifra de bloco ou uma cifra de fluxo. Clique nos botões para saber mais sobre esses dois modos de cifra.

**Cifras de bloco**

**As cifras de bloco** transformam um bloco de texto simples de comprimento fixo em um bloco comum de texto cifrado de 64 ou 128 bits. As cifras de bloco comuns incluem DES com um tamanho de bloco de 64 bits e AES com um tamanho de bloco de 128 bits.

A figura mostra uma mensagem de texto simples sendo criptografada em blocos de 64 bits.

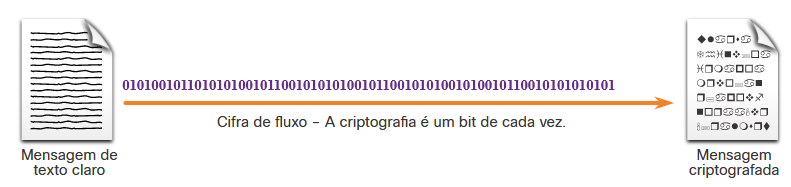


Mensagem de texto claroMensagem criptografada64 bits64 bits64 bitsCifra de blocos – A criptografia é realizada em blocos de 64 bits.1100101 em branco em branco

Algoritmos de criptografia simétrica mais conhecidos são descritos na tabela.

**Cifras de fluxo**

**As cifras de fluxo** criptografam o texto simples um byte ou um bit de cada vez. As cifras de fluxo são basicamente uma cifra de bloco com um tamanho de bloco de um byte ou bit. As cifras de fluxo geralmente são mais rápidas do que as cifras de bloco porque os dados são criptografados continuamente. Exemplos de cifras de fluxo incluem RC4 e A5, que é usado para criptografar comunicações de telefone celular GSM.



| **Algoritmos de criptografia simétrica** | **Descrição** |
| --- | --- |
| **Data Encryption Standard (DES)** | Este é um algoritmo de criptografia simétrica legado. Ele usa um comprimento de chave curto que o torna inseguro para a maioria dos usos atuais. |
| **3DES (Triple DES)** | O é o substituto do DES e repete o processo do algoritmo DES três vezes. Deve ser evitado, se possível, uma vez que está programado para ser aposentado em 2023. Se implementado, use durações de chave muito curtas. |
| **AES (Advanced Encryption Standard)** | AES é um algoritmo de criptografia simétrica popular e recomendado. Ele oferece combinações de chaves de 128, 192 ou 256 bits para criptografar blocos de dados de 128, 192 ou 256 bits. |
| **Software-Optimized Encryption Algorithm (SEAL)** | SEAL é uma alternativa mais rápida de algoritmo de criptografia simétrica para AES. SEAL é uma cifra de fluxo que usa uma chave de criptografia de 160 bits e tem um impacto menor na CPU em comparação com outros algoritmos baseados em software. |
| **Algoritmos da série Rivest ciphers (RC)** | Este algoritmo foi desenvolvido por Ron Rivest. Diversas variações foram desenvolvidas, mas o RC4 foi o mais prevalente em uso. RC4 é uma cifra de fluxo usada para proteger o tráfego da web. Verificou-se que tem múltiplas vulnerabilidades que o tornaram inseguro. O RC4 não deve ser utilizado. |

21.2.3

## Criptografia Assimétrica

Os algoritmos assimétricos, também chamados algoritmos de chave pública, são projetados para que a chave usada para criptografia seja diferente da chave usada para descriptografia, conforme mostrado na figura. A chave de descriptografia não pode, em uma quantidade razoável de tempo, ser calculada a partir da chave de criptografia e vice-versa.

A figura mostra um exemplo de criptografia assimétrica em que a chave de criptografia é diferente da chave de descriptografia.

### Exemplo de criptografia assimétrica



Chave de criptografiaTexto claroCriptografadoCriptografiaTexto claroDescriptografiaChave de descriptografia

Algoritmos assimétricos usam uma chave pública e uma chave privada. Ambas as chaves são capazes do processo de criptografia, mas a chave emparelhada complementar é necessária para descriptografia. O processo também é reversível. Os dados criptografados com a chave pública requerem a chave privada para descriptografar. Algoritmos assimétricos alcançam confidencialidade e autenticidade usando este processo.

Como nenhuma das partes possui um segredo compartilhado, é necessário usar comprimentos de chave muito longos. A criptografia assimétrica pode usar comprimentos de chave entre 512 e 4.096 bits. Comprimentos de chave maiores ou iguais a 2.048 bits podem ser confiáveis, enquanto comprimentos de chave de 1.024 ou menores são considerados insuficientes.

Exemplos de protocolos que usam algoritmos de chave assimétrica incluem:

* **Internet Key Exchange (IKE) -** é um componente fundamental das redes virtuais privadas IPsec (VPNs).
* **Secure Socket Layer (SSL) -**Agora isso é implementado como TLS (Transport Layer Security) padrão da IETF.
* **Secure Shell (SSH) -** Este protocolo fornece uma conexão segura de acesso remoto a dispositivos de rede.
* **Pretty Good Privacy (PGP) -** Este programa de computador fornece privacidade e autenticação criptográficas. É frequentemente usado para aumentar a segurança das comunicações por email.

Os algoritmos assimétricos são substancialmente mais lentos que os algoritmos simétricos. Seu design é baseado em problemas computacionais, como fatorar números extremamente grandes ou calcular logaritmos discretos de números extremamente grandes.

Por serem lentos, algoritmos assimétricos geralmente são usados em mecanismos criptográficos de baixo volume, como assinaturas digitais e troca de chaves. No entanto, o gerenciamento de chaves de algoritmos assimétricos tende a ser mais simples que os algoritmos simétricos, porque geralmente uma das duas chaves de criptografia ou descriptografia pode ser tornada pública.

Exemplos comuns de algoritmos de criptografia assimétrica são descritos na tabela.

| **Algoritmo de criptografia assimétrica** | **comprimento da chave** | **Descrição** |
| --- | --- | --- |
| **Diffie-Hellman (DH)** | 512, 1024, 2048, 3072, 4096 | O algoritmo Diffie-Hellman permite que duas partes concordem com uma chave que elas podem usar para criptografar as mensagens que desejam enviar uma para a outra. A segurança desse algoritmo depende da suposição de que é fácil aumentar um número para uma determinada potência, mas difícil calcular qual potência foi usada, dado o número e o resultado. |
| **Padrão de Assinatura Digital (DSS) e Algoritmo de Assinatura Digital (DSA)** | 512 - 1024 | O DSS especifica o DSA como o algoritmo para assinaturas digitais. DSA é um algoritmo de chave pública baseado no esquema de assinatura ElGamal. A velocidade de criação da assinatura é semelhante ao RSA, mas é 10 a 40 vezes mais lenta para verificação. |
| **Algoritmos de criptografia Rivest, Shamir e Adleman (RSA)** | 512 até 2048 | O RSA é para criptografia de chave pública que se baseia na dificuldade atual de fatorar números muito grandes. É o primeiro algoritmo conhecido por ser adequado para assinatura, bem como criptografia. É amplamente utilizado em protocolos de comércio eletrônico e acredita-se ser seguro, dadas chaves suficientemente longas e o uso de implementações atualizadas. |
| **EIGamal** | 512 - 1024 | Um algoritmo de criptografia de chave assimétrica para criptografia de chave pública que se baseia no contrato de chave Diffie-Hellman. Uma desvantagem do sistema ElGamal é que a mensagem criptografada se torna muito grande, aproximadamente o dobro do tamanho da mensagem original e, por esse motivo, é usada apenas para mensagens pequenas, como chaves secretas. |
| **Técnicas de curva elíptica** | 224 ou superior | A criptografia de curva elíptica pode ser usada para adaptar muitos algoritmos criptográficos, como Diffie-Hellman ou ElGamal. A principal vantagem da criptografia de curva elíptica é que as chaves podem ser muito menores. |

21.2.4

## Criptografia Assimétrica - Confidencialidade

Algoritmos assimétricos são usados para fornecer confidencialidade sem pré-compartilhar uma senha. O objetivo de confidencialidade dos algoritmos assimétricos é iniciado quando o processo de criptografia é iniciado com a chave pública.

O processo pode ser resumido usando a fórmula:

**Chave pública (criptografar) + chave privada (descriptografar) = confidencialidade**

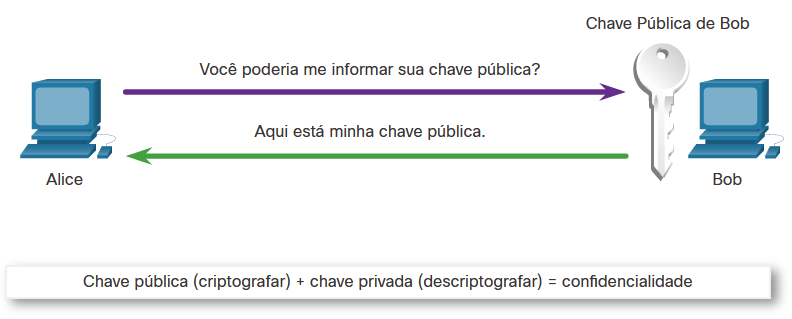
Quando a chave pública é usada para criptografar os dados, a chave privada deve ser usada para descriptografar os dados. Apenas um host tem a chave privada; portanto, a confidencialidade é alcançada.

Se a chave privada estiver comprometida, outro par de chaves deve ser gerado para substituir a chave comprometida.

Clique nos botões para ver como as chaves privadas e públicas podem ser usadas para fornecer confidencialidade à troca de dados entre Bob e Alice.

**Alice solicita e obtém a chave pública de Bob.**

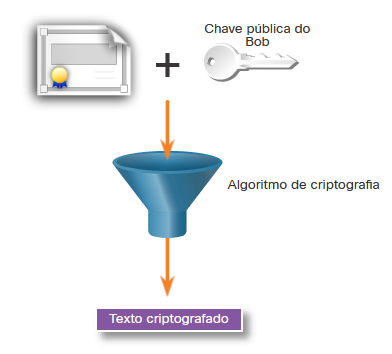
A figura mostra o computador alice à esquerda e o computador bob à direita. O computador Bob tem uma chave à esquerda com as palavras chave pública do Bob. Uma flecha vai da Alice P C para o Bob PC com as palavras, posso pegar sua chave pública, por favor? Outra linha com uma flecha indo de Bob para Alice com as palavras aqui é minha chave pública. Na parte inferior: chave pública (criptografar) + chave privada (descriptografar) = confidencialidade.



Chave pública (criptografar) + chave privada (descriptografar) = confidencialidadeVocê poderia me informar sua chave pública?Aqui está minha chave pública.AliceBobChave Pública de Bob

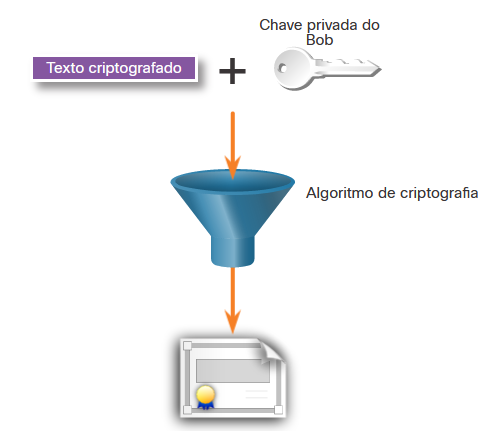
**Alice usa a chave pública**

Alice usa a chave pública de Bob para criptografar uma mensagem usando um algoritmo acordado. Alice envia a mensagem criptografada para Bob.



**Bob descriptografa mensagem com chave privada**

Bob então usa sua chave privada para descriptografar a mensagem. Como Bob é o único com a chave privada, a mensagem de Alice só pode ser descriptografada por Bob e, portanto, a confidencialidade é alcançada.



21.2.5

## Criptografia assimétrica - autenticação

O objetivo de autenticação de algoritmos assimétricos é iniciado quando o processo de criptografia é iniciado com a chave privada.

O processo pode ser resumido usando a fórmula:

**Chave privada (criptografar) + chave pública (descriptografar) = autenticação**

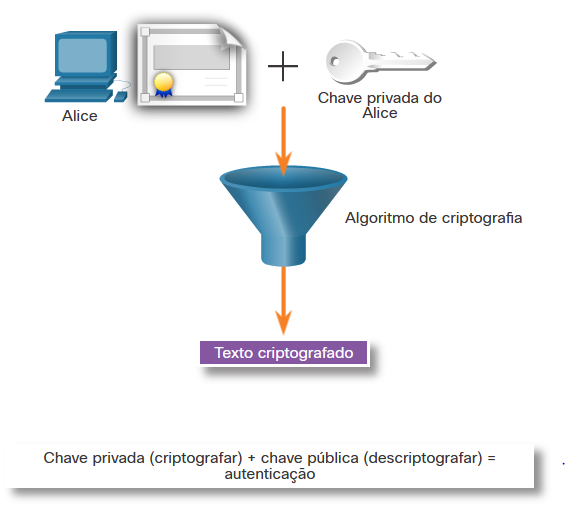
Quando a chave privada é usada para criptografar os dados, a chave pública correspondente deve ser usada para descriptografar os dados. Como apenas um host tem a chave privada, somente esse host poderia ter criptografado a mensagem, fornecendo autenticação do remetente. Normalmente, nenhuma tentativa é feita para preservar o sigilo da chave pública, portanto, qualquer número de hosts pode descriptografar a mensagem. Quando um host descriptografa uma mensagem com êxito usando uma chave pública, é confiável que a chave privada criptografou a mensagem, o que verifica quem é o remetente. Esta é uma forma de autenticação.

Clique nos botões para ver como as chaves privadas e públicas podem ser usadas para fornecer autenticação para a troca de dados entre Bob e Alice.

**Alice usa sua chave privada**

Alice criptografa uma mensagem usando sua chave privada. Alice envia a mensagem criptografada para Bob. Bob precisa autenticar que a mensagem realmente veio de Alice.

A figura mostra o computador alice com um certificado ao lado dele, um sinal de adição e uma chave rotulada chave privada de Alice com uma seta indo para um funil rotulado algoritmo de criptografia. Uma seta sai do funil para uma caixa de texto que lê texto criptografado. Na parte inferior estão as palavras chave privada (criptografar) + chave pública (descriptografar) = autenticação.



Texto criptografadoChave privada do AliceAlgoritmo de criptografiaChave privada (criptografar) + chave pública (descriptografar) = autenticaçãoAlice

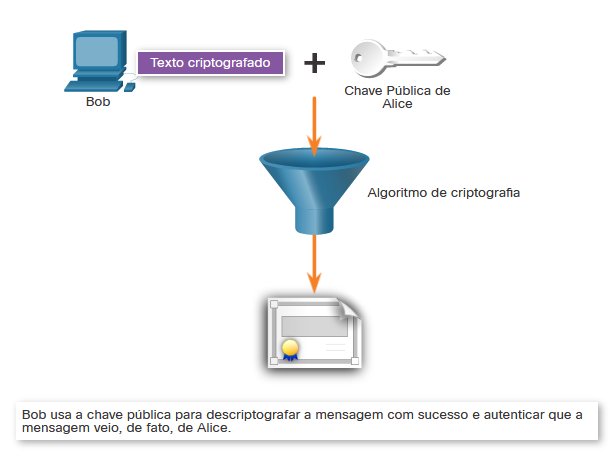
**Bob solicita a chave pública**

Para autenticar a mensagem, Bob solicita a chave pública de Alice.



**Bob descriptografa usando a chave pública**

Bob usa a chave pública de Alice para descriptografar a mensagem.



21.2.6

## Criptografia assimétrica - integridade

Combinar os dois processos de criptografia assimétrica fornece confidencialidade, autenticação e integridade da mensagem.

O exemplo a seguir será usado para ilustrar esse processo. Neste exemplo, uma mensagem será cifrada usando a chave pública de Bob e um hash cifrado será criptografado usando a chave privada de Alice para fornecer confidencialidade, autenticidade e integridade.

**Alice usa a chave publica de Bob**

Alice quer enviar uma mensagem para Bob assegurando que só Bob pode ler o documento. Em outras palavras, Alice quer garantir a confidencialidade da mensagem. Alice usa a chave pública de Bob para cifrar a mensagem. Só Bob será capaz de decifrá-lo usando sua chave privada.

A figura mostra o computador alice com um pedaço de papel em texto simples ao lado dele, um sinal de adição e uma chave rotulada chave pública de Bob com uma seta entrando em um algoritmo de criptografia rotulado funil. Uma seta sai do funil para uma caixa de texto que lê texto criptografado.

+

**Alice criptografa um hash usando sua chave privada**

Alice também quer garantir a autenticação e integridade da mensagem. A autenticação garante a Bob que o documento foi enviado por Alice, e a integridade garante que ele não foi modificado Alice usa sua chave privada para cifrar um hash da mensagem. Alice envia a mensagem criptografada com seu hash criptografado para Bob.

**Bob usa a chave pública de Alice para descriptografar o HASH**

Bob usa a chave pública de Alice para verificar se a mensagem não foi modificada. O hash recebido é igual ao hash determinado localmente com base na chave pública de Alice. Além disso, isso verifica se Alice é definitivamente o remetente da mensagem porque ninguém mais tem a chave privada de Alice.

**Bob usa sua chave privada para descriptogafar a mensagem**

Bob usa sua chave privada para decifrar a mensagem.

21.2.7

## Diffie-Hellman

Diffie-Hellman (DH) é um algoritmo matemático assimétrico que permite que dois computadores gerem um segredo compartilhado idêntico sem terem se comunicado antes. A nova chave compartilhada nunca é realmente trocada entre o remetente e o destinatário. No entanto, como as duas partes o conhecem, a chave pode ser usada por um algoritmo de criptografia para criptografar o tráfego entre os dois sistemas.

Aqui estão dois exemplos de casos em que DH é comumente usado:

* Os dados são trocados usando uma VPN IPsec
* Dados SSH são trocados

Para ajudar a ilustrar como o DH opera, consulte a figura.

A figura ilustra como o algoritmo Diffie-Hellman funciona usando cores. Suponha que Alice e Bob concordaram em começar com 50 mililitros (50ml) de tinta amarela. Alice adiciona 50 ml de tinta vermelha à tinta amarela para criar uma quantidade de 100 ml de tinta laranja. Bob mistura seus 50 ml de tinta amarela com 50 ml de tinta azul para criar 100 ml de tinta verde. Alice envia Bob seus 100 ml de tinta de cor laranja e Bob envia Alice sua 100 ml de tinta de cor verde. Alice, em seguida, passa a adicionar mais 50 ml de sua tinta vermelha aos 100 ml de tinta verde de Bob para criar 150 ml de tinta marrom. Bob mistura mais 50 ml de tinta azul com os 100 ml de tinta laranja de Alice para criar 150 ml da mesma cor cor marrom tinta que Alice criou.

=

Concordou em coresCor secreta de AliceCor Pública de AliceCor Pública de BobCor secreta de AliceCor Final de AliceAliceConcordou em coresCor Secreta de BobCor Pública de BobCor Pública de AliceCor privada de BobCor Final de BobBob

As cores na figura serão usadas em vez de números longos complexos para simplificar o processo de contrato de chave DH. A troca de chaves DH começa com Alice e Bob concordando com uma cor comum arbitrária que não precisa ser mantida em segredo. A cor combinada em nosso exemplo é amarelo.

Em seguida, Alice e Bob selecionarão uma cor secreta. Alice escolheu vermelho enquanto Bob escolheu azul. Essas cores secretas nunca serão compartilhadas com ninguém. A cor secreta representa a chave privada secreta escolhida de cada parte.

Alice e Bob agora misturam a cor comum compartilhada (amarelo) com suas respectivas cores secretas para produzir uma cor pública. Portanto, Alice vai misturar o amarelo com sua cor vermelha para produzir uma cor pública de laranja. Bob irá misturar o amarelo e o azul para produzir uma cor pública de verde.

Alice envia sua cor pública (laranja) para Bob e Bob envia sua cor pública (verde) para Alice.

Alice e Bob misturam a cor que receberam com a sua própria cor secreta original (vermelho para Alice e azul para Bob). O resultado é uma mistura final de cor marrom que é idêntica à mistura de cor final do parceiro. A cor marrom representa a chave secreta compartilhada resultante entre Bob e Alice.

A segurança do DH se baseia-se no fato de que ele usa números muito grandes em seus cálculos. Por exemplo, um número DH 1024 bits é aproximadamente igual a um número decimal de 309 dígitos. Considerando que um bilhão é 10 dígitos decimais (1.000.000.000), pode-se facilmente imaginar a complexidade de trabalhar não com um, mas com vários números decimais de 309 dígitos.

Diffie-Hellman usa diferentes grupos DH para determinar a força da chave que é usada no processo de acordo de chave. Os números de grupo mais altos são mais seguros, mas exigem tempo adicional para calcular a chave. O seguinte identifica os grupos DH suportados pelo Cisco IOS Software e seu valor de número primo associado:

* DH Group 1: 768 bits
* DH Group 2: 1024 bits
* DH Group 5: 1536 bits
* DH Group 14: 2048 bits
* DH Group 15: 3072 bits
* DH Group 16: 4096 bits

**Nota**: Um acordo de chave DH também pode ser baseado em criptografia de curva elíptica. Os grupos DH 19, 20 e 24, que são baseados em criptografia de curva elíptica, também são suportados pelo Cisco IOS Software.

Infelizmente, os sistemas de chave assimétrica são extremamente lentos para qualquer tipo de criptografia em massa. É por isso que é comum criptografar a maior parte do tráfego usando um algoritmo simétrico, como 3DES ou AES, e usar o algoritmo DH para criar chaves que serão usadas pelo algoritmo de criptografia.

21.2.8

## Vídeo - Criptografia

Assista ao vídeo para saber mais sobre Criptografia.

# Criptografia de chave pública

21.3.1

## Uso de assinaturas digitais

As assinaturas digitais são uma técnica matemática usada para fornecer autenticidade, integridade e não repúdio. As assinaturas digitais têm propriedades específicas que permitem autenticação de entidade e integridade de dados. Além disso, as assinaturas digitais fornecem não repúdio da transação. Em outras palavras, a assinatura digital serve como prova legal de que o intercâmbio de dados ocorreu. As assinaturas digitais usam criptografia assimétrica.

Clique nos botões para explorar as propriedades das assinaturas digitais.

Autenticidade - A assinatura não pode ser falsificada e fornece prova de que o signatário, e ninguém mais, assinou o documento.

Inalterável - Após assinar um documento, ele não pode ser alterado

Não reutilizável - A assinatura do documento não pode ser transferida para outro documento.

Não repudiado - O documento assinado é considerado o mesmo que um documento físico. A assinatura é a prova de que o documento foi assinado pela pessoa real.

As assinaturas digitais são comumente usadas nas duas situações a seguir:

1. **Assinatura de código** — Isso é usado para fins de autenticação e integridade de dados. A assinatura de código é usada para verificar a integridade dos arquivos executáveis baixados do site de um fornecedor. Ele também usa certificados digitais assinados para autenticar e verificar a identidade do site que é a origem dos arquivos.
2. **Certificados digitais** - são semelhantes a um cartão de identificação virtual e usados para autenticar a identidade do sistema com o site de um fornecedor e estabelecer uma conexão criptografada para trocar dados confidenciais.

Existem três algoritmos DSS (Digital Signature Standard) que são usados para gerar e verificar assinaturas digitais:

* **Algoritmo de Assinatura Digital (DSA)** - DSA é o padrão original para gerar pares de chaves públicas e privadas e para gerar e verificar assinaturas digitais.
* **Rivest-Shamir Adelman Algoritmo (RSA)** - RSA é um algoritmo assimétrico que é comumente usado para gerar e verificar assinaturas digitais.
* **Elliptic Curve Digital Signature Algoritmo (ECDSA)** - O ECDSA é uma variante mais recente do DSA e fornece autenticação de assinatura digital e não repúdio com os benefícios adicionais da eficiência computacional, tamanhos de assinatura pequenos e largura de banda mínima.

Na década de 1990, a RSE Security Inc. começou a publicar padrões de criptografia de chave pública (PKCS). Havia 15 PKCS, embora 1 tenha sido retirado a partir do momento em que esta escrita foi escrita. A RSE publicou estes padrões porque possuíam as patentes aos padrões e desejavam promovê-los. Os PKCS não são padrões do setor, mas são bem reconhecidos no setor de segurança e recentemente começaram a se tornar relevantes para organizações de padrões como o grupo de trabalho IETF e PKIX.

21.3.2

## Assinaturas digitais para assinatura de código

As assinaturas digitais são comumente usadas para garantir a autenticidade e integridade do código de software. Os arquivos executáveis são empacotados em um envelope assinado digitalmente, o que permite ao usuário final verificar a assinatura antes de instalar o software.

Assinar digitalmente o código fornece várias garantias sobre o código:

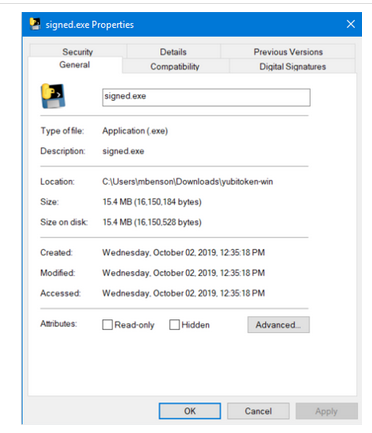
* O código é autêntico e é realmente originado pela editora.
* O código não foi modificado desde que saiu do editor do software.
* A editora publicou inegavelmente o código. Isso fornece não repúdio do ato de publicação.

A Publicação 140-3 do FIPS (Federal Information Processing Standard) do Governo dos EUA especifica que o software disponível para download na internet deve ser assinado e verificado digitalmente. O objetivo do software assinado digitalmente é garantir que o software não foi adulterado e que ele foi originado da fonte confiável, conforme reivindicado. As assinaturas digitais servem como verificação de que o código não foi adulterado por agentes da ameaça e o código malicioso não foi inserido no arquivo por terceiros.

Clique nos botões para acessar as propriedades de um arquivo que tenha um certificado assinado digitalmente.

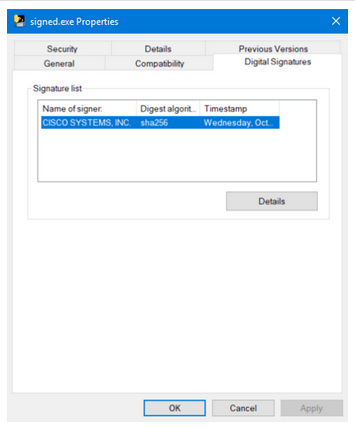
**Propriedades do arquivo**

Este arquivo executável foi baixado da Internet. O arquivo contém uma ferramenta de software da Cisco Systems.



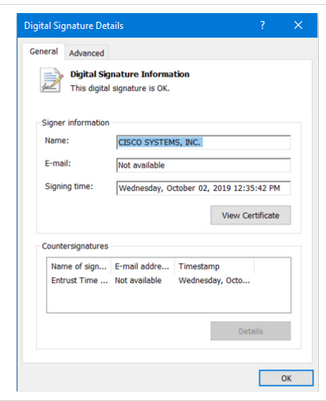
**Assinaturas digitais**

Clicar na guia Digital Signatures revela que o arquivo é de uma organização confiável, o Cisco Systems Inc. O Digest do arquivo foi criado com o algoritmo SHA256. A data em que o arquivo foi assinado também é fornecida. Clicar em Details abre a janela Detalhes de assinaturas digitais.



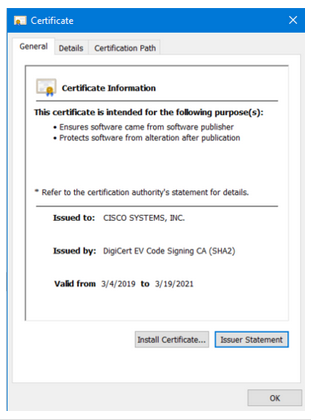
**Detalhes de assinaturas digitais**

A janela Detalhes da assinatura digital revela que o arquivo foi assinado pela Cisco Systems, Inc em outubro de 2019. Isso foi verificado pela contrassinatura fornecida pela Entrust Time Stamping Authority no mesmo dia em que foi assinado pela Cisco. Clique View Certificate para ver os detalhes do próprio certificado.



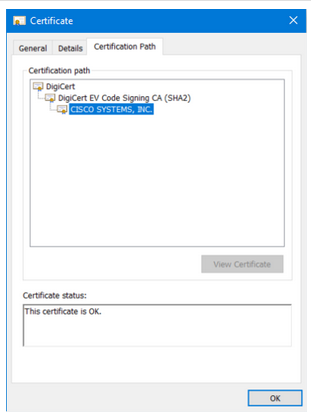
**Informações de cerificado**

A guia General fornece os propósitos do certificado, que o certificado foi emitido e que emitiu o certificado. Ele também exibe o período para o qual o certificado é válido. Certificados inválidos podem impedir que o arquivo seja executado.



**Caminho de certificação**

Clique na guia Certification Path para ver o arquivo foi assinado pelos sistemas Cisco, conforme verificado para Digicert. Em alguns casos, uma entidade adicional pode verificar independentemente o certificado.

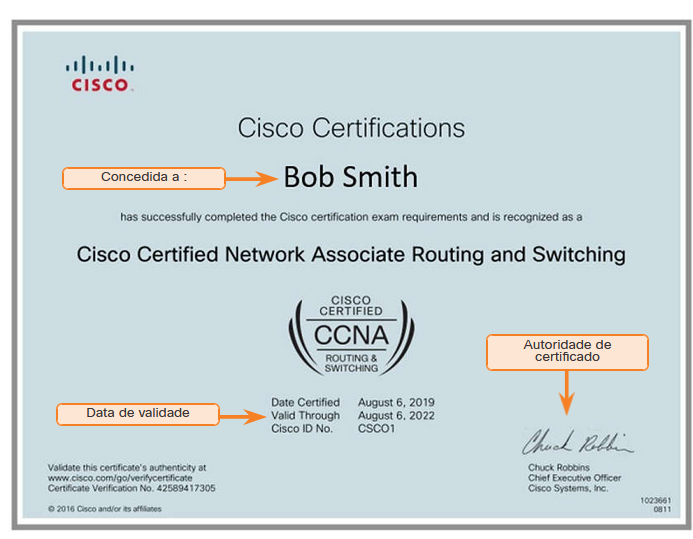


21.3.3

**Assinaturas digitais para certificados digitais**

Um certificado digital é equivalente a um passaporte eletrônico. Ele permite que usuários, hosts e organizações troquem informações com segurança pela Internet. Especificamente, um certificado digital é usado para autenticar e verificar se um usuário que está enviando uma mensagem é quem afirma ser. Os certificados digitais também podem ser usados para fornecer confidencialidade ao receptor com os meios de criptografar uma resposta.

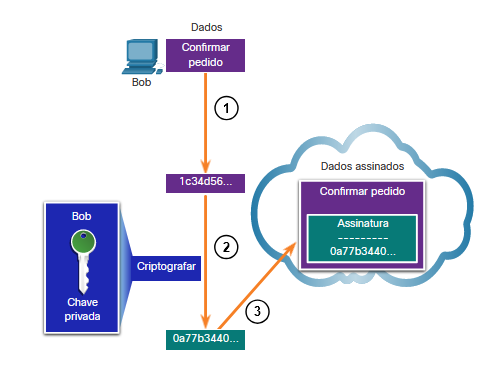
Os certificados digitais são semelhantes aos certificados físicos. Por exemplo, o certificado Cisco Certified Network Associate Security (CCNA-S) em papel na figura identifica para quem o certificado foi emitido, quem autorizou o certificado e por quanto tempo o certificado é válido. Os certificados digitais também fornecem informações semelhantes.



O certificado digital verifica de forma independente uma identidade. Assinaturas digitais são usadas para verificar se um artefato, como um arquivo ou mensagem, é enviado pelo indivíduo verificado. Em outras palavras, um certificado verifica a identidade, uma assinatura verifica se algo vem dessa identidade.

Esse cenário ajudará você a entender como uma assinatura digital é usada. Bob está confirmando um pedido com Alice. Alice está encomendando do site do Bob. Alice se conectou com o site de Bob, e depois que o certificado foi verificado, o certificado de Bob é armazenado no site de Alice. O certificado contém a chave pública de Bob. A chave pública é usada para verificar a assinatura digital do Bob.

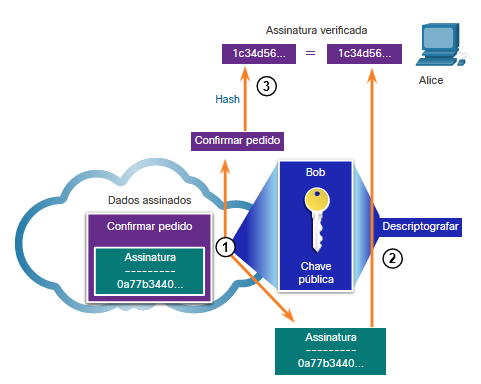
Consulte a figura para ver como a assinatura digital é usada.



Bob confirma a ordem e seu computador cria um hash da confirmação. O computador criptografa o hash com a chave privada do Bob. O hash criptografado, que é a assinatura digital, é anexado ao documento. A confirmação do pedido é então enviada para Alice através da internet.

Quando Alice recebe a assinatura digital, ocorre o seguinte processo.

A figura mostra a mesma nuvem com dados assinados e confirmar a caixa de encomenda da última figura com um número circulado que tem a chave pública de Bob e descriptografar nela, um hash e uma assinatura verificada caixas que levam ao computador de Alice.



1. O dispositivo receptor de Alice aceita a confirmação do pedido com a assinatura digital e obtém a chave pública de Bob.
2. O computador de Alice descodifica a assinatura usando a chave pública de Bob. Esta etapa revela o valor de hash assumido do dispositivo de envio.
3. O computador de Alice cria um hash do documento recebido, sem sua assinatura, e compara esse hash com o hash de assinatura descriptografado. Se os hashes corresponderem, o documento é autêntico. Isso significa que a confirmação foi enviada por Bob e que ela não mudou desde que foi assinada

# Autoridades e o Sistema de Confiança PKI

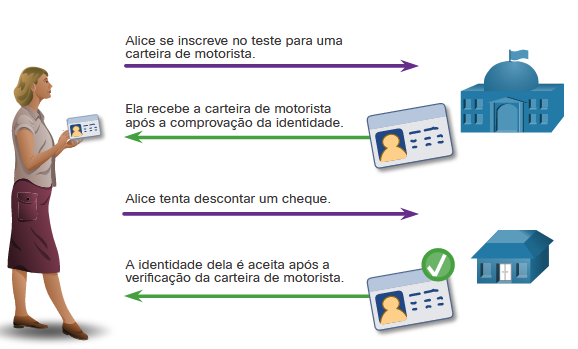
21.4.1

## Gerenciamento de Chave Pública

O tráfego da Internet consiste no tráfego entre duas partes. Ao estabelecer uma conexão assimétrica entre dois hosts, os hosts trocarão suas informações de chave pública.

Um certificado SSL é um certificado digital que confirma a identidade de um domínio de site. Para implementar SSL em seu site, você compra um certificado SSL para seu domínio de um provedor de Certificado SSL. O terceiro de confiança faz uma investigação aprofundada antes da emissão das credenciais. Após essa investigação aprofundada, o terceiro emite credenciais (ou seja, certificado digital) que são difíceis de falsificar. Desse ponto em diante, todos os indivíduos que confiam no terceiro simplesmente aceitam as credenciais que o terceiro emite. Quando os computadores tentam se conectar a um site via HTTPS, o navegador verifica o certificado de segurança do site e verifica se ele é válido e originado com uma autoridade de certificação confiável. Isso valida que a identificação do site é verdadeira. O certificado é salvo localmente pelo navegador da Web e, em seguida, é usado em transações subsequentes. A chave pública do site está incluída no certificado e é usada para verificar futuras comunicações entre o site e o cliente.

Esses terceiros confiáveis fornecem serviços semelhantes aos escritórios de licenciamento governamentais. A figura ilustra como uma carteira de motorista é análoga a um certificado digital.



A Infraestrutura de Chave Pública (PKI) consiste em especificações, sistemas e ferramentas que são usados para criar, gerenciar, distribuir, usar, armazenar e revogar certificados digitais. A autoridade de certificação (CA) é uma organização que cria certificados digitais vinculando uma chave pública a uma identificação confirmada, como um site ou indivíduo. O PKI é um sistema complexo que é projetado para proteger identidades digitais contra hackers até mesmo os atores de ameaças mais sofisticados ou estados-nação.

Alguns exemplos de Autoridades de Certificação são IDentrust, DigiCert, Sectigo, GlobalSign e GoDaddy. Essas CAs cobram por seus serviços. Let's Encrypt é uma CA sem fins lucrativos que oferece certificados gratuitamente.

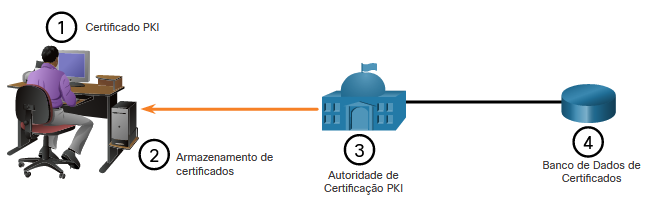
21.4.2

**A infraestrutura de chave pública**

A PKI é necessária para oferecer suporte à distribuição em larga escala e à identificação de chaves de criptografia públicas. A estrutura PKI facilita uma relação de confiança altamente escalável.

Consiste em hardware, software, pessoas, políticas e procedimentos necessários para criar, gerenciar, armazenar, distribuir e revogar certificados digitais.

A figura mostra os principais elementos da PKI.



A figura mostra um usuário em um pc com as palavras P K I certificado acima dele e um número circulado. Há um número circulado 2 ao lado do computador com o armazenamento de certificados palavras. À direita do usuário há um círculo três ícone de edifício público rotulado autoridade de certificação PKI e à direita disso é um círculo quatro e um cilindro rotulado banco de dados certificado.

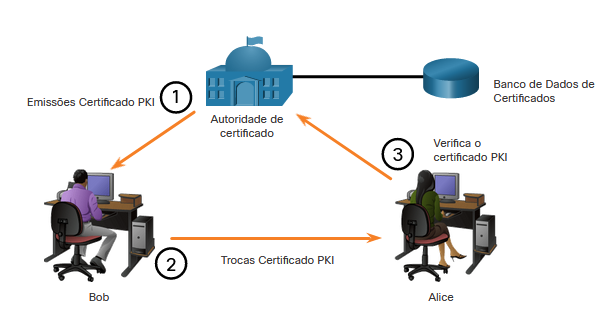
Os certificados PKI contêm a chave pública de uma entidade ou de um indivíduo, a sua finalidade, a autoridade de certificação (AC) que validou e emitiu o certificado, o intervalo de datas durante o qual o certificado é válido e o algoritmo usado para criar a assinatura.

O armazenamento de certificados reside em um computador local e armazena certificados emitidos e chaves privadas.

O Certificado de Autoridade PKI (CA) é um terceiro confiável que emite certificados PKI para entidades e indivíduos após verificar sua identidade. Ele assina esses certificados usando sua chave privada.

O banco de dados de certificados armazena todos os certificados aprovados pela autoridade de certificação.

A figura seguinte mostra como os elementos da PKI interoperam:



Neste exemplo, Bob recebeu seu certificado digital da CA. Este certificado é usado sempre que Bob se comunica com outras partes.

Bob se comunica com Alice.

Quando Alice recebe o certificado digital de Bob, ela se comunica com a autoridade de certificação confiável para validar a identidade de Bob.

A figura mostra um ícone de banco de dados de certificados no canto superior direito com uma linha conectando-o a um ícone de edifício público rotulado autoridade de certificação e o número um circulado ao lado dele com as palavras emite o certificado PKI. Uma seta vai para um usuário de computador rotulado bob que tem o número circulado dois ao lado dele uma seta que leva ao usuário de computador alice com as palavras trocas PKI certificado. Acima do computador alice estão as palavras verifica o certificado PKI, um número circulado 3, e uma seta os pontos de volta para a autoridade de certificação.

Autoridade de certificadoBanco de Dados de CertificadosBobAliceTrocas Certificado PKIVerifica o certificado PKIEmissões Certificado PKI

Emissões Certificado PKI. Bob inicialmente solicita um certificado da autoridade de certificação. A autoridade de certificação autentica Bob e armazena o certificado PKI de Bob no banco de dados de certificados.

Trocas Certificado PKI. Bob se comunica com Alice usando seu certificado PKI.

Verifica o certificado PKI. Alice se comunica com o C A confiável usando a chave pública da CA. O CA refere-se ao banco de dados de certificados para validar o certificado PKI de Bob.

Observação: nem todos os certificados PKI são recebidos diretamente de uma autoridade de certificação. Uma autoridade de registro (RA) é uma autoridade de certificação subordinada e é certificada por uma autoridade de certificação raiz para emitir certificados para usos específicos.

21.4.3

## O Sistema de Autoridades PKI

Muitos fornecedores fornecem servidores da CA como um serviço gerenciado ou como um produto de usuário final. Alguns desses fornecedores incluem Symantec Group (VeriSign), Comodo, Go Daddy Group, GlobalSign e DigiCert, entre outros.

As organizações também podem implementar PKIs privadas usando o Microsoft Server ou Open SSL.

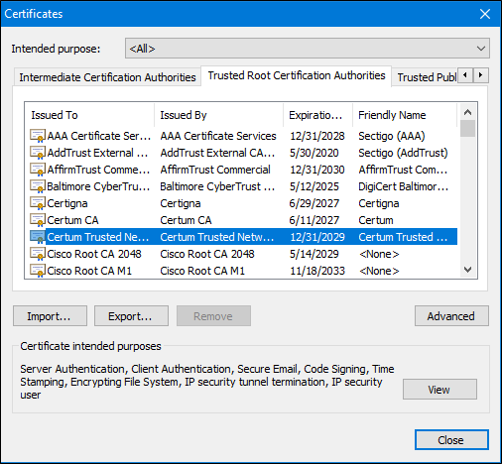
As autoridades de certificação, especialmente aquelas que são terceirizadas, emitem certificados baseados em classes que determinam a confiabilidade de um certificado.

A tabela fornece uma descrição das classes. O número de classe é determinado pelo rigor do procedimento que verificou a identidade do titular quando o certificado foi emitido. Quanto maior o número da classe, mais confiável será o certificado. Portanto, um certificado de classe 5 é confiável muito mais do que um certificado de classe inferior.

| **Classe** | **Descrição** |
| --- | --- |
| 0 | Usado para testes em situações em que não foram realizadas verificações. |
| 1 | Usado por indivíduos que exigem verificação de e-mail. |
| 2 | Usado por organizações para as quais a prova de identidade é necessária. |
| 3 | Usado para servidores e assinatura de software. A autoridade certificadora procede à verificação e verificação independentes da identidade e da autoridade. |
| 4 | Usado para transações comerciais on-line entre empresas. |
| 5 | Usado para organizações privadas ou segurança do governo. |

Por exemplo, um certificado de classe 1 pode exigir uma resposta por e-mail do titular para confirmar que deseja se inscrever. Este tipo de confirmação é uma autenticação fraca do titular. Para um certificado de classe 3 ou 4, o futuro titular deve provar a identidade e autenticar a chave pública aparecendo pessoalmente com pelo menos dois documentos de identificação oficiais.

Algumas chaves públicas da CA são pré-carregadas, como as listadas em navegadores da Web. A figura exibe vários certificados VeriSign contidos no armazenamento de certificados no host. Quaisquer certificados assinados por qualquer uma das autoridades de certificação na lista serão vistos pelo navegador como legítimos e serão confiáveis automaticamente.



**Nota**: Uma empresa também pode implementar PKI para uso interno. A PKI pode ser usada para autenticar funcionários que estão acessando a rede. Nesse caso, a empresa é sua própria CA.

21.4.4

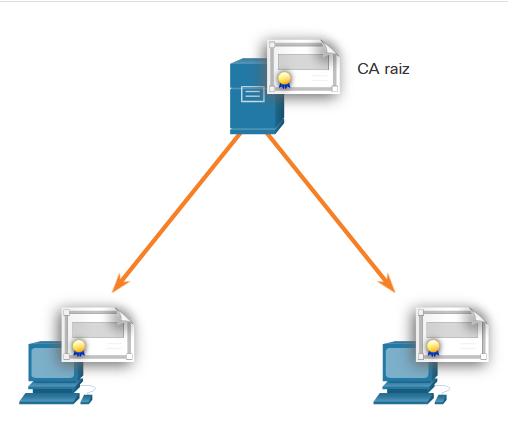
## O Sistema de Confiança PKI

PKIs podem formar diferentes topologias de confiança. O mais simples é a topologia PKI de raiz única.

Como mostrado na figura abaixo, uma única autoridade de certificação, chamada de CA raiz, emite todos os certificados para os usuários finais, que geralmente estão dentro da mesma organização. O benefício desta abordagem é a sua simplicidade. No entanto, é difícil dimensionar para um ambiente grande porque requer uma administração estritamente centralizada, o que cria um único ponto de falha.

A figura mostra um servidor rotulado Road C A com um certificado ao lado dele. Existem duas flechas cada vez apontando para um computador. Cada computador também tem um certificado ao lado dele.

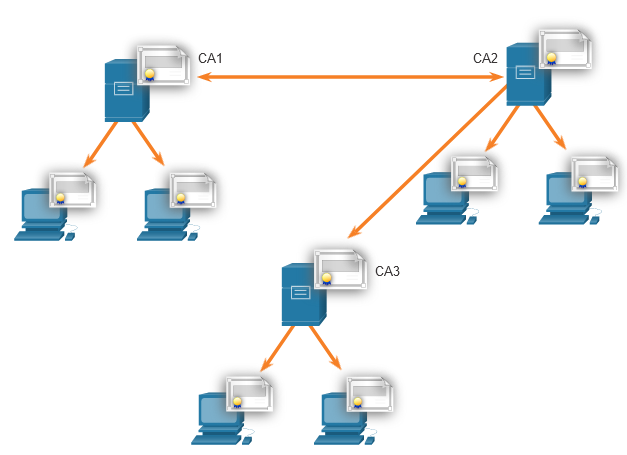
### Topologia PKI de raiz única

Em redes maiores, as CAs PKI podem ser vinculadas usando duas arquiteturas básicas:

**Topologias de AC certificadas cruzadas** - Conforme mostrado na figura abaixo, este é um modelo ponto a ponto no qual as ACs individuais estabelecem relações de confiança com outras ACs através da certificação cruzada de certificados de AC. Os usuários em ambos os domínios da CA também têm a certeza de que podem confiar uns nos outros. Isso fornece redundância e elimina o ponto único de falha.

A figura mostra a mesma configuração como a topologia de PKI de raiz única anterior, mas é rotulado CA 1. Há uma seta de duas vias entre esta topologia e outra da mesma topologia rotulada CA 2. Um ponto de seta da Topologia CA 2para outra da mesma topologia rotulada CA 3.

### CA com certificação cruzada



**Topologias de CA hierárquicas** - Conforme mostrado na figura abaixo, a CA de nível mais alto é chamada de CA raiz. Ele pode emitir certificados para usuários finais e para uma autoridade de certificação subordinada. As subCAs podem ser criadas para suportar várias unidades de negócios, domínios ou comunidades de confiança. A autoridade de certificação raiz mantém a “comunidade de confiança” estabelecida garantindo que cada entidade na hierarquia esteja em conformidade com um conjunto mínimo de práticas. Os benefícios dessa topologia incluem maior escalabilidade e capacidade de gerenciamento. Esta topologia funciona bem na maioria das grandes organizações. No entanto, pode ser difícil determinar a cadeia do processo de assinatura.

Uma topologia hierárquica e de certificação cruzada pode ser combinada para criar uma infraestrutura híbrida. Um exemplo seria quando duas comunidades hierárquicas querem certificar-se entre si para que os membros de cada comunidade confiem uns nos outros.

A figura mostra um servidor rotulado Road C A com um certificado ao lado dele. Há duas flechas, cada um apontando para um subordinado c a cada um com uma topologia PKI de raiz única.

### CA hierárquica



## Interoperabilidade de diferentes fornecedores de PKI

A interoperabilidade entre uma PKI e seus serviços de suporte, como o Lightweight Directory Access Protocol (LDAP) e diretórios X.500, é uma preocupação porque muitos fornecedores de CA propuseram e implementaram soluções proprietárias em vez de aguardar o desenvolvimento de padrões.

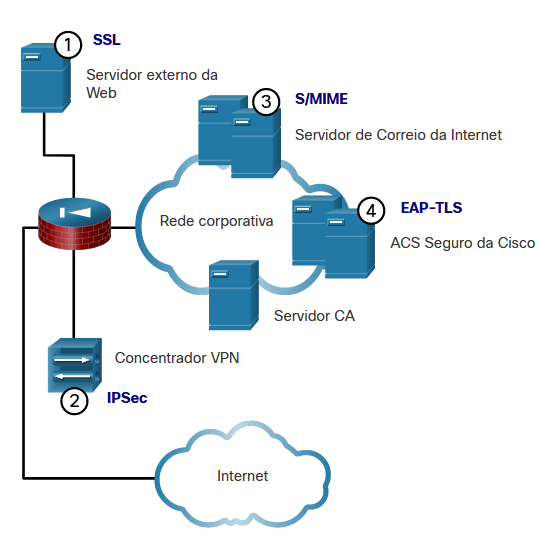
**Observação**: LDAP e X.500 são protocolos usados para consultar um serviço de diretório, como o Microsoft Active Directory, para verificar um nome de usuário e senha.

Para resolver esse problema de interoperabilidade, o IETF publicou o Internet X.509 Public Key Infrastructure Policy and Certification Practices Framework (RFC 2527). O padrão X.509 versão 3 (X.509 v3) define o formato de um certificado digital.

Consulte a figura para obter mais informações sobre aplicativos X.509 v3. Como mostrado na figura, o formato X.509 já é amplamente utilizado na infra-estrutura da internet.

A figura mostra um servidor Web externo rotulado com o número circulado 1 e S S L que se conecta a um firewall. O firewall tem outra conexão com um concentrador V P N abaixo dele rotulado com o número 2 circulado e as palavras I P s e c. O firewall tem uma terceira conexão com uma nuvem rotulada Internet. O firewall tem outra conexão com uma nuvem de rede corporativa que inclui um servidor CA, um servidor de email da Internet que tem o número circulado 3 e S/MIME ao lado dele, e servidores que têm o Cisco Secure ACS ao lado dele e o número circulado quatro palavras EAP - TLS ao lado dele.

### Aplicações x.509v3



InternetRede corporativaConcentrador VPNServidor externo da WebServidor de Correio da InternetACS Seguro da CiscoServidor CASSLS/MIMEEAP-TLSIPSec

1. **SSL** - Servidores Web seguros Use X.509.v3 para autenticação do site nos protocolos SSL e TLS, enquanto os navegadores da Web usam X.509V3 para implementar certificados de cliente HTTPS. SSL é a autenticação baseada em certificado mais utilizada.
2. **IPsec** - IPsec VPNS usa certificados X.509 quando a autenticação baseada em RSA é usada para a Intercâmbio de chaves da Internet (IKE).
3. **S/MIME** - Os agentes de correio do usuário que suportam proteção de correio com o protocolo Secure / Multipurpose Internet Mail Extensions (S / MIME) usam certificados X.509.
4. **EAP-TLS** - Os switches da Cisco podem usar certificados para autenticar dispositivos finais que se conectam a portas de LAN usando 802.1x entre os dispositivos adjacentes. A autenticação pode ser proxy para um ACS central por meio do Extensible Authentication Protocol with TLS (EAP-TLS).

21.4.6

## Inscrição, autenticação e revogação de certificados

A primeira etapa no procedimento de autenticação da autoridade de certificação é obter com segurança uma cópia da chave pública da autoridade de certificação. Todos os sistemas que utilizam a PKI devem ter a chave pública da autoridade de certificação, que é chamada de certificado autoassinado. A chave pública da autoridade de certificação verifica todos os certificados emitidos pela autoridade de certificação e é vital para o bom funcionamento da PKI.

**Observação**: somente uma autoridade de certificação raiz pode emitir um certificado autoassinado reconhecido ou verificado por outras autoridades de certificação dentro da PKI.

Para muitos sistemas, como navegadores da Web, a distribuição de certificados de CA é processada automaticamente. O navegador da Web vem pré-instalado com um conjunto de certificados raiz de CA públicos. As organizações e seus domínios do site enviam seus certificados públicos para os visitantes do site. As autoridades de certificação e os registradores de domínio de certificado criam e distribuem certificados privados e públicos para clientes que compram certificados.

O processo de registro de certificado é usado por um sistema host para se inscrever com uma PKI. Para fazer isso, os certificados de CA são recuperados em banda através de uma rede e a autenticação é feita fora de banda (OOB) usando o telefone. O registro do sistema com a PKI entra em contato com uma autoridade de certificação para solicitar e obter um certificado de identidade digital para si mesmo e para obter o certificado autoassinado da autoridade de certificação. O estágio final verifica se o certificado da autoridade de certificação foi autêntico e é executado usando um método fora de banda, como o sistema de telefone antigo simples (POTS), para obter a impressão digital do certificado de identidade da autoridade de certificação válido.

A autenticação não requer mais a presença do servidor da autoridade de certificação e cada usuário troca seus certificados contendo chaves públicas.

Os certificados devem, por vezes, ser revogados. Por exemplo, um certificado digital pode ser revogado se a chave for comprometida ou se não for mais necessário.

Aqui estão dois dos métodos mais comuns de revogação:

* **Lista de revogação de certificados (CRL)** - Uma lista de números de série de certificados revogados que foram invalidados porque expiraram. As entidades PKI pesquisam regularmente o repositório CRL para receber a CRL atual.
* **Protocolo de Status de Certificado Online (OCSP)** - Um protocolo de Internet usado para consultar um servidor OCSP para o status de revogação de um certificado digital X.509. As informações de revogação são imediatamente enviadas para um banco de dados on-line.

21.4.7

## Laboratório — Armazenamento de autoridade de certificação

Neste laboratório, você completará os seguintes objetivos:

* Certificados Confiáveis pelo Seu Navegador
* Verificando o Man-In-Mi

# Aplicações e impactos da criptografia

21.5.1

## Aplicações PKI

Onde a PKI pode ser usada por uma empresa? O seguinte fornece uma pequena lista de usos comuns de PKIs:

* Autenticação de peer baseada em certificado SSL/TLS
* Proteja o tráfego de rede usando VPNs IPsec
* Tráfego da web HTTPS
* Controle o acesso à rede usando a autenticação 802.1x
* E-mail seguro usando o protocolo S/MIME
* Mensagens instantâneas seguras
* Aprovar e autorizar aplicativos com assinatura de código
* Proteja os dados do usuário com o sistema de arquivos de criptografia (EFS)
* Implementar autenticação de dois fatores com cartões inteligentes
* Protegendo dispositivos de armazenamento USB

21.5.2

## Transações de rede criptográfica

Um analista de segurança deve ser capaz de reconhecer e resolver possíveis problemas relacionados à permissão de soluções relacionadas à PKI na rede corporativa.

Considere como o aumento do tráfego SSL/TLS representa um grande risco de segurança para as empresas porque o tráfego é criptografado e não pode ser interceptado e monitorado por meios normais. Os usuários podem introduzir malware ou vazar informações confidenciais através de uma conexão SSL/TLS.

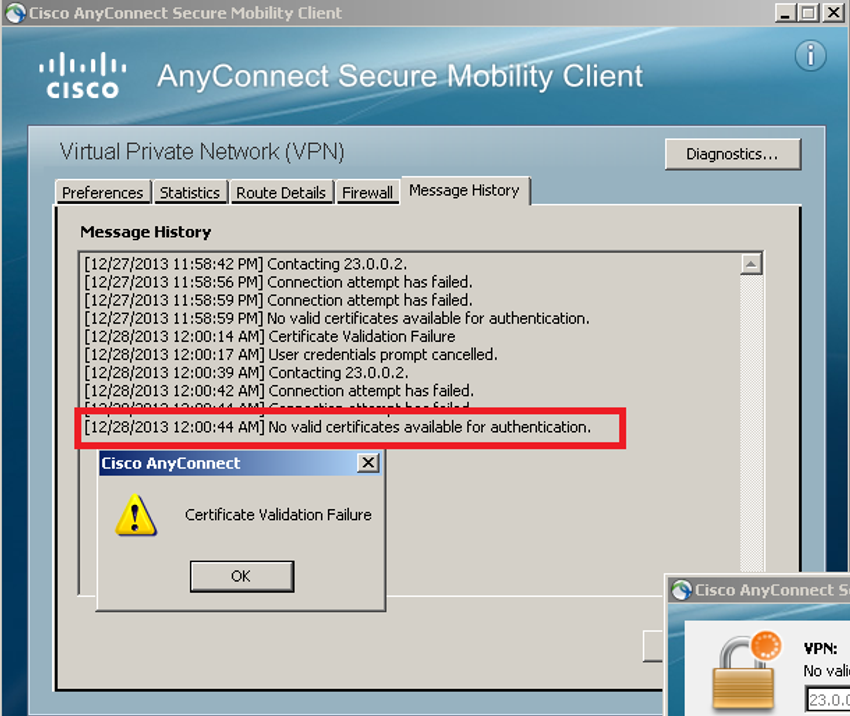
Os atores de ameaças podem usar SSL/TLS para introduzir violações de conformidade regulatória, vírus, malware, perda de dados e tentativas de intrusão em uma rede.

Outros problemas relacionados a SSL/TLS podem estar associados à validação do certificado de um servidor Web. Quando isso ocorre, os navegadores da Web exibirão um aviso de segurança. Os problemas relacionados à PKI associados a avisos de segurança incluem:

* **Faixa de datas de validade** - Os certificados X.509v3 especificam datas “não antes” e “não depois”. Se a data atual estiver fora do intervalo, o navegador da Web exibirá uma mensagem. Os certificados expirados podem simplesmente ser o resultado da supervisão do administrador, mas também podem refletir condições mais graves.
* **Erro de validação de assinatura** - Se um navegador não puder validar a assinatura no certificado, não há garantia de que a chave pública no certificado seja autêntica. A validação de assinatura falhará se o certificado raiz da hierarquia da autoridade de certificação não estiver disponível no armazenamento de certificados do navegador.

A figura mostra um exemplo de erro de validação de assinatura com o Cisco AnyConnect Mobility VPN Client.

### Erro de validação de assinatura



Alguns desses problemas podem ser evitados devido ao fato de que os protocolos SSL/TLS são extensíveis e modulares. Isto é conhecido como um conjunto de cifras. Os principais componentes do conjunto de cifras são o MAC (Message Authentication Code Algoritmo), o algoritmo de criptografia, o algoritmo de troca de chaves e o algoritmo de autenticação. Estes podem ser alterados sem substituir todo o protocolo. Isso é muito útil porque os diferentes algoritmos continuam a evoluir. À medida que a criptoanálise continua a revelar falhas nesses algoritmos, o conjunto de cifras pode ser atualizado para corrigir essas falhas. Quando as versões de protocolo dentro do conjunto de cifras mudam, o número de versão do SSL/TLS também muda.

21.5.3

## Criptografia e monitoramento de segurança

O monitoramento de rede torna-se mais desafiador quando os pacotes são criptografados. No entanto, os analistas de segurança devem estar cientes desses desafios e enfrentá-los da melhor forma possível. Por exemplo, quando VPNs site a site são usadas, o IPS deve ser posicionado para que ele possa monitorar o tráfego não criptografado.

No entanto, o aumento do uso de HTTPS na rede empresarial introduz novos desafios. Como o HTTPS introduz tráfego HTTP criptografado de ponta a ponta (via TLS/SSL), não é tão fácil espiar o tráfego do usuário.

Os analistas de segurança devem saber como contornar e resolver esses problemas. Aqui está uma lista de algumas das coisas que um analista de segurança pode fazer:

* Configure regras para distinguir entre tráfego SSL e não-SSL, tráfego SSL HTTPS e não-HTTPS.
* Melhore a segurança através da validação de certificados de servidor utilizando CRLs e OCSP.
* Implemente proteção antimalware e filtragem de URL de conteúdo HTTPS.
* Implante um Cisco SSL Appliance para descriptografar o tráfego SSL e enviá-lo para dispositivos IPS (Intrusion Prevention System, sistema de prevenção de intrusões) para identificar riscos normalmente ocultos pelo SSL.

A criptografia é dinâmica e está sempre mudando. Um analista de segurança deve manter um bom entendimento de algoritmos criptográficos e operações para ser capaz de investigar incidentes de segurança relacionados à criptografia.

Há duas maneiras principais em que a criptografia afeta as investigações de segurança. Primeiro, os ataques podem ser direcionados especificamente para os próprios algoritmos de criptografia. Após o algoritmo ter sido rachado e o invasor obter as chaves, todos os dados criptografados que foram capturados podem ser descriptografados pelo invasor e lidos, expondo assim dados privados. Em segundo lugar, a investigação de segurança também é afetada porque os dados podem ser escondidos à vista, encriptando-os. Por exemplo, o tráfego de comando e controle criptografado com TLS/SSL provavelmente não pode ser visto por um firewall. O tráfego de comando e controle entre um servidor de comando e controle e um computador infectado em uma rede segura não pode ser interrompido se não puder ser visto e compreendido. O invasor seria capaz de continuar usando comandos criptografados para infectar mais computadores e, possivelmente, criar uma botnet. Esse tipo de tráfego pode ser detectado descriptografando o tráfego e comparando-o com assinaturas de ataque conhecidas ou detectando tráfego TLS/SSL anômalo. Isso é muito difícil e demorado, ou um processo de acerto ou erro.

# Resumo de criptografia

21.6.1

## O que aprendi neste módulo?

**Comunicações seguras**

As organizações devem fornecer suporte para proteger os dados conforme eles trafegam pelos links. Existem quatro elementos de comunicações seguras: integridade de dados, autenticação de origem, confidencialidade de dados e não repúdio de dados. A criptografia pode ser usada em praticamente qualquer lugar em que haja comunicação de dados. Hashes são usados para verificar e garantir a integridade dos dados. O hash é baseado em uma função matemática unilateral que é relativamente fácil de calcular, mas significativamente mais difícil de reverter. A função de hash criptográfico também pode ser usada para verificar a integridade. Uma função hash leva um bloco variável de dados binários, chamado de mensagem, e produz uma representação condensada de comprimento fixo, chamado de hash. Existem quatro funções hash bem conhecidas: MD5 com 128-bit digest, SHA-1, SHA-2 e SHA-3. Embora o hashing possa ser usado para detectar alterações acidentais, ele não pode ser usado para proteger contra alterações deliberadas feitas por um agente de ameaça. Hashing é vulnerável a ataques homem-em-meio. Para fornecer autenticação de integridade e origem, é necessário algo mais. Para adicionar autenticação à garantia de integridade, use um código de mensagem com chave (HMAC). HMACs usam uma chave secreta adicional como entrada à função hash.

**Sigilo dos dados**

Existem duas classes de criptografia que são usadas para fornecer confidencialidade de dados: assimétrica e simétrica. Essas duas classes diferem na maneira como usam as chaves. Algoritmos de criptografia simétricos, como DES, 3DES e AES são baseados na premissa de que cada parte que se comunica conhece a chave pré-compartilhada. A confidencialidade dos dados também pode ser garantida usando algoritmos assimétricos, incluindo Rivest, Shamir e Aldeman (RSA) e PKI. Os algoritmos simétricos são comumente usados com o tráfego VPN porque usam menos recursos da CPU do que os algoritmos de criptografia assimétricos. Algoritmos de criptografia simétrica às vezes são classificados como cifras de bloco ou de fluxo. Os algoritmos assimétricos (algoritmos de chave pública) são projetados de forma que a chave usada para criptografia seja diferente da chave usada para criptografia. Os algoritmos assimétricos usam uma chave pública e uma chave privada. Exemplos de protocolos que usam algoritmos de chave assimétrica incluem IKE, SSL, SSH e PGP. Exemplos comuns de algoritmos de criptografia assimétrica incluem técnicas DSS, DSA, RSA, EiGamal e curvas elípticas. Algoritmos assimétricos são usados para fornecer confidencialidade sem pré-compartilhar uma senha. O processo é resumido usando esta fórmula: Chave pública (Criptografar) + Chave Privada (Decrypt) = Confidencialidade. O objetivo de autenticação de um algoritmo assimétrico é iniciado quando o processo de criptografia é iniciado com a chave privada. O processo pode ser resumido com esta fórmula: Chave Privada (Criptografar) + Chave Pública (Decrypt) = Autenticação. Combinar os dois processos de criptografia assimétrica fornece confidencialidade, autenticação e integridade da mensagem. Diffie-Hellman (DH) é um algoritmo de equação matemática assimétrica que permite que dois computadores gerem uma chave secreta compartilhada idêntica sem se comunicar antes. Dois exemplos de instâncias quando DH é usado são quando os dados são trocas usando uma VPN IPsec e quando dados SSH são trocados.

**Criptografia de chave pública**

As assinaturas digitais são uma técnica matemática usada para fornecer três serviços básicos de segurança: autenticidade, integridade e não repúdio. Propriedades da assinatura digital são que eles são autênticos, inalteráveis, não reutilizáveis e não repudiados. As assinaturas digitais são comumente usadas nas duas situações a seguir: assinatura de código e certificados digitais. Existem três algoritmos DSS (Digital Signature Standard) que são usados para gerar e verificar assinaturas digitais: Digital Signature Algorithm (DSA), Revet-Shamir Adelman Algoritmo (RSA) e Elliptical Curve Digital Signature Algoritmo (ECDSA). Assinar digitalmente o código fornece garantias sobre o código do software: o código é autêntico e é realmente originado pelo editor, o código não foi modificado desde que deixou o editor do software e o editor publicou inegavelmente o código. Um certificado digital é equivalente a um passaporte eletrônico. Ele permite que usuários, hosts e organizações troquem informações com segurança pela Internet. Especificamente, um certificado digital é usado para autenticar e verificar se um usuário que está enviando uma mensagem é quem afirma ser.

**Autoridades e o Sistema de Confiança PKI**

Ao estabelecer uma conexão segura entre dois hosts, os hosts trocarão suas informações de chave pública. Existem terceiros confiáveis na Internet que validam a autenticidade dessas chaves públicas usando certificados digitais. A Infraestrutura de Chave Pública (PKI) consiste em especificações, sistemas e ferramentas que são usados para criar, gerenciar, distribuir, usar, armazenar e revogar certificados digitais. A PKI é necessária para oferecer suporte à distribuição em larga escala de chaves de criptografia públicas. A estrutura PKI facilita uma relação de confiança altamente escalável. Muitos fornecedores fornecem servidores da CA como um serviço gerenciado ou como um produto de usuário final. Alguns desses fornecedores incluem Symantec Group (VeriSign), Comodo, Go Daddy Group, GlobalSign e DigiCert, entre outros. O número de classe (0 completo 5) é determinado pelo rigor do procedimento que verificou a identidade do titular quando o certificado foi emitido, sendo cinco o mais alto. PKIs podem formar diferentes topologias de confiança. O mais simples é a topologia PKI de raiz única. A interoperabilidade entre a PKI e seus serviços de suporte é uma preocupação porque muitos fornecedores de CA propuseram e implementaram uma solução proprietária em vez de aguardar o desenvolvimento de padrões. Para resolver o problema de interoperabilidade, o IETF publicou o Internet X>509 Public Key Infrastructure Certificate Policy and Certification Framework (RFC 2527).

**Aplicações e impactos da criptografia**

Há muitos usos comuns de PKIs, incluindo alguns listados aqui: autenticação de ponto baseada em certificado SSL/TLS, tráfego da Web HTTPS, mensagens instantâneas seguras e proteção de dispositivos de armazenamento USB. Um analista de segurança deve ser capaz de reconhecer e resolver possíveis problemas relacionados à permissão de soluções relacionadas à PI na rede empresarial. Por exemplo, os atores de ameaças podem usar SSL/TSL para introduzir violações de conformidade normativa, vírus, malware, perda de dados e tentativas de intrusão na rede. Outros problemas relacionados com SSL/TSL podem estar associados à validação do certificado do servidor web. Problemas relacionados à PKI que estão associados a avisos de segurança incluem intervalo de datas de validade e validação de assinatura. Alguns desses problemas podem ser evitados devido ao fato de que os protocolos SSL/TSL são extensíveis e modulares. Isto é conhecido como o conjunto de cifras. Os principais componentes do conjunto de cifras são o MAC (Message Authentication Code Algoritmo), o algoritmo de criptografia, o algoritmo de troca de chaves e o algoritmo de autenticação. A criptografia é dinâmica e está sempre mudando. Você deve manter um bom entendimento de algoritmos e operações para ser capaz de investigar incidentes de segurança relacionados à criptografia. As comunicações criptografadas podem tornar as cargas de dados de segurança de rede ilegíveis pelos analistas de segurança cibernética. A criptografia pode ser usada para ocultar o comando de malware e controlar o tráfego entre hosts infectados e os servidores de comando e controle. Além disso, o malware pode ser ocultado por criptografia e os dados podem ser criptografados durante a exfiltração, dificultando a detecção.

21.6.2

# Introdução

22.0.1

## Por que devo cursar este módulo?

Os endpoints são qualquer dispositivo que se comunica com qualquer outro dispositivo em uma rede. Isso inclui milhares de PCs, impressoras, servidores e outros dispositivos encontrados em uma rede grande. Cada ponto de extremidade é vulnerável a ataques. Como todos esses endpoints podem ser protegidos, e podemos saber se algum deles foi comprometido por um ator de ameaças ou malware? Este módulo descreve várias tecnologias e métodos de proteção de terminais, que se combinam para ajudar a proteger melhor sua casa e sua organização.

22.0.2

## O que vou aprender neste módulo?

**Título do módulo:** Proteção de endpoints

**Objetivo do Módulo:** Explique como um site de análise de malware gera um relatório de análise de malware.

| **Tópico** | **Objetivo do Tópico** |
| --- | --- |
| Proteção Antimalware | Explicar os métodos de mitigação de malware. |
| Prevenção de intrusão baseada em host | Explicar entradas de log IPS / IDS baseadas em host |
| Segurança de aplicações | Explique como um sandbox é usado para analisar malware |

# Proteção Antimalware

22.1.1

## Ameaças de endpoint

O termo “endpoint” é definido de várias maneiras. Para fins deste curso, podemos definir endpoints como hosts na rede que podem acessar ou ser acessados por outros hosts na rede. Isso obviamente inclui computadores e servidores, no entanto muitos outros dispositivos também podem acessar a rede. Com o rápido crescimento da Internet das Coisas (IoT), outros tipos de dispositivos são agora endpoints na rede. Isso inclui câmeras de segurança em rede, controladores e até mesmo lâmpadas e aparelhos. Cada ponto de extremidade é potencialmente uma forma de software malicioso obter acesso a uma rede. Além disso, as novas tecnologias, como a nuvem, expandem os limites das redes empresariais para incluir locais na Internet pelos quais as empresas não são responsáveis.

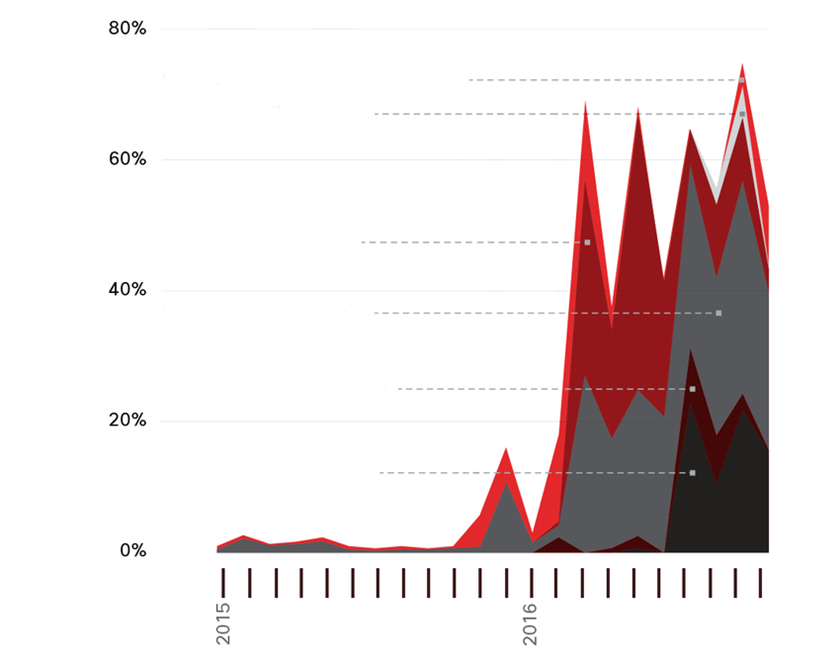
Dispositivos que acessam redes remotamente através de VPNs também são endpoints que precisam ser considerados. Esses endpoints podem injetar malware na rede VPN a partir da rede pública.

Os pontos a seguir resumem algumas das razões pelas quais o malware continua sendo um grande desafio:

* De acordo com pesquisas da Cybersecurity Ventures, até 2021 uma nova organização será vítima de um ataque de ransomware a cada 11 segundos.
* Os ataques de ransomware custarão à economia global US$6 trilhões por ano até 2021.
* Em 2018, 8 milhões de tentativas de roubar recursos do sistema usando malware de criptografia foram observadas.
* De 2016 até o início de 2017, o volume global de spam aumentou drasticamente. De 8 a 10 por cento deste spam pode ser considerado malicioso, como mostrado na figura.
* Em 2020, prevê-se que o número médio de ataques cibernéticos por dispositivo macOS aumentará de 4.8 em 2018 para 14,2 em 2020.
* Vários tipos comuns de malware foram encontrados para alterar significativamente os recursos em menos de 24 horas, a fim de evitar a detecção.

A Figura 1 mostra os e-mails por segundo enviados de 2012 a 2016 e o aumento de 0 ponto 5 K de volta em 20 12 para mais de 3 K em 20 16. A Figura 2 mostra a porcentagem da extensão total de cerca de 0 por cento em janeiro de 2015 para como em 2016 quase 15% contém pontos maliciosos w s f, e 25% contém ponto malicioso d o c m, perto de 40% contém arquivos zip ponto maliciosos, quase 50% contém arquivos de ponto j s maliciosos, quase 70 por cento contém arquivos de ponto malicioso percentual contém arquivos maliciosos ponto h t a, e mais de 70% contém anexos mal-intencionados baseados na pesquisa de segurança da Cisco.

### Porcentagem de Spam



Porcentagem do Spam totalContendo anexos mal-intencionadosContém maliciosos.HTAContém Malicious.jsContém Malicious.zipContém maliciosos.docmContém Malicious.wsfFonte: Cisco Security Research

22.1.2

## Segurança de endpoints

A mídia de notícias geralmente cobre ataques de rede externa em redes corporativas. Estes são alguns exemplos de tais ataques:

* Ataques DoS na rede de uma organização para degradar ou mesmo interromper o acesso público a ela
* Violação do servidor web de uma organização para desfigurar sua presença na Web
* Violação de servidores de dados e hosts de uma organização para roubar informações confidenciais

Vários dispositivos de segurança de rede são necessários para proteger o perímetro da rede contra acesso externo. Como mostrado na figura, esses dispositivos podem incluir um roteador reforçado que está fornecendo serviços VPN, um firewall de próxima geração (ASA, na figura), um appliance IPS e um servidor de serviços de autenticação, autorização e contabilidade (AAA) (Servidor AAA, na figura).

A figura retrata uma rede de área do campus. Uma nuvem representando a Internet é conectado a um roteador, rotulado VPN. O roteador VPN está conectado a um ASA firewall. O firewall tem duas conexões adicionais; uma para um IPS e outro para um interruptor. O switch está conectado a um servidor DHCP, servidor de e-mail, e ESA/WSA. O IPS está conectado a um switch multicamadas. O switch multicamadas tem uma conexão a um servidor AAA, bem como a duas camadas 2 e um para outro switch multicamada. O segundo switch multicamadas também tem conexões com os mesmos switches de camada 2, criando redundância. Abaixo do switches de camada 2 são três laptops e três pcs que são rotulados como hosts.

**Rede do campus**InternetServidor AAAASA  
FirewallSwitches de camada 3VPNIPSESA/WSASwitches da Camada 2Servidor DHCPServidor de e-mailServidor WebHosts

No entanto, muitos ataques se originam de dentro da rede. Portanto, proteger uma LAN interna é quase tão importante quanto proteger o perímetro externo da rede. Sem uma LAN segura, os usuários de uma organização ainda são suscetíveis a ameaças de rede e paralisações que podem afetar diretamente a produtividade e a margem de lucro de uma organização. Depois que um host interno é infiltrado, ele pode se tornar um ponto de partida para um invasor obter acesso a dispositivos críticos do sistema, como servidores e informações confidenciais.

Especificamente, há dois elementos LAN internos para proteger:

* **Endpoints** - Os hosts geralmente consistem em laptops, desktops, impressoras, servidores e telefones IP, todos eles suscetíveis a ataques relacionados a malware.
* **Infraestrutura de rede** - Os dispositivos de infraestrutura LAN interconectam pontos de extremidade e geralmente incluem switches, dispositivos sem fio e dispositivos de telefonia IP. A maioria desses dispositivos é suscetível a ataques relacionados à LAN, incluindo ataques de estouro de tabela de endereços MAC, ataques de falsificação, ataques relacionados a DHCP, ataques de tempestade de LAN, ataques de manipulação de STP e ataques de VLAN.

Este módulo se concentra na proteção de endpoints.

22.1.3

## Proteção contra malware baseada em host

O perímetro da rede está sempre se expandindo. As pessoas acessam recursos de rede corporativa com dispositivos móveis que usam tecnologias de acesso remoto, como VPN. Esses mesmos dispositivos também são usados em redes públicas e domésticas não seguras ou minimamente protegidas. Software antimalware/antivírus baseado em host e firewalls baseados em host são usados para proteger esses dispositivos.

**Software antivírus / antimalware**

Este é um software instalado em um host para detectar e mitigar vírus e malware. Exemplos são o Windows Defender Virus & Threat Protection, Cisco AMP for Endpoints, Norton Security, McAfee, Trend Micro e outros. Programas antimalware podem detectar vírus usando três abordagens diferentes:

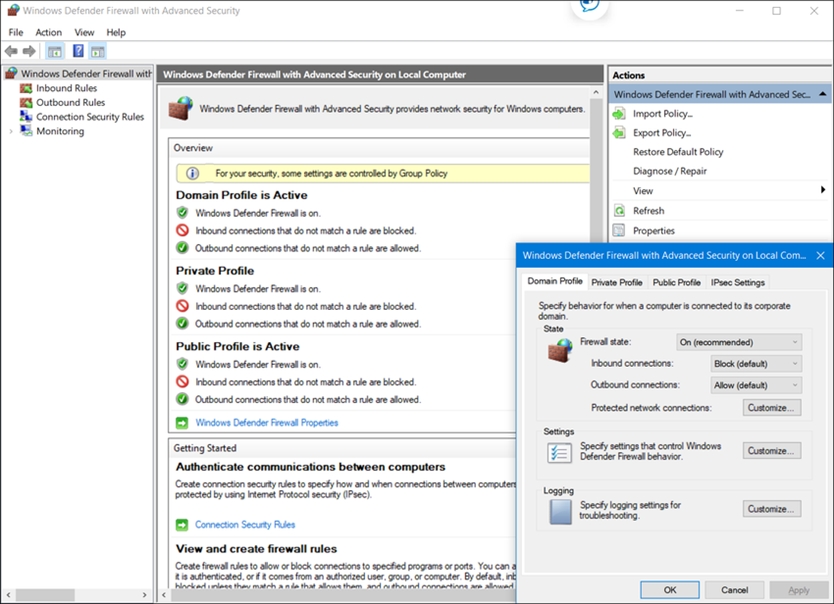
* **Baseado em assinaturas** — Essa abordagem reconhece várias características de arquivos de malware conhecidos.
* **Baseado em heurística** — Essa abordagem reconhece recursos gerais compartilhados por vários tipos de malware.
* **Baseado em comportamento** — Essa abordagem emprega análise de comportamento suspeito.

Muitos programas antivírus são capazes de fornecer proteção em tempo real analisando dados conforme eles são usados pelo endpoint. Esses programas também verificam se há malware existente que pode ter entrado no sistema antes de ser reconhecível em tempo real.

A proteção antivírus baseada em host também é conhecida como baseada em agentes. O antivírus baseado em agente é executado em todas as máquinas protegidas. A proteção antivírus sem agente executa verificações em hosts a partir de um sistema centralizado. Os sistemas sem agente tornaram-se populares para ambientes virtualizados nos quais várias instâncias de SO estão sendo executadas em um host simultaneamente. Antivírus baseado em agente executado em cada sistema virtualizado pode ser um sério desperdício de recursos do sistema. O antivírus sem agente para hosts virtuais envolve o uso de um appliance virtual de segurança especial que executa tarefas de varredura otimizadas nos hosts virtuais. Um exemplo disso é o vShield da VMware.

**Firewall de host**

Este software está instalado em um host. Restringe conexões de entrada e saída a conexões iniciadas somente por esse host. Alguns softwares de firewall também podem impedir que um host se infecte e impedir que hosts infectados espalhem malware para outros hosts. Esta função está incluída em alguns sistemas operacionais. Por exemplo, o Windows inclui o Firewall do Windows Defender com Segurança Avançada, conforme mostrado na figura.



Outras soluções são produzidas por outras empresas ou organizações. As ferramentas Linux iptables e TCP Wrappers são exemplos. Os firewalls baseados em host são discutidos com mais detalhes posteriormente neste módulo.

**Host-based Security Suites**

Recomenda-se instalar um conjunto de produtos de segurança baseado em host em redes domésticas e também em redes comerciais. Esses pacotes de segurança baseados em host incluem antivírus, anti-phishing, navegação segura, sistema de prevenção de intrusões baseado em host e recursos de firewall. Essas várias medidas de segurança fornecem uma defesa em camadas que protegerá contra as ameaças mais comuns.

Além da funcionalidade de proteção fornecida pelos produtos de segurança baseados em host é a função de telemetria. A maioria dos softwares de segurança baseados em host inclui funcionalidade de registro robusta que é essencial para operações de segurança cibernética. Alguns programas de segurança baseados em host enviarão logs para um local central para análise.

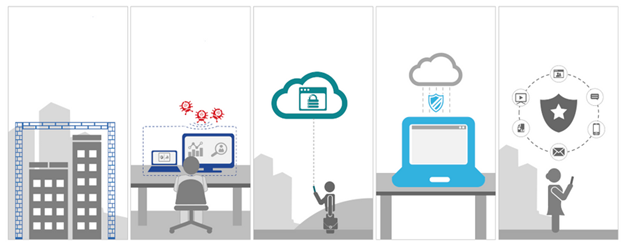
Há muitos programas e pacotes de segurança baseados em host disponíveis para usuários e empresas. O laboratório de testes independente AV-TEST fornece análises de alta qualidade de proteções baseadas em host, bem como informações sobre muitos outros produtos de segurança.

Pesquise na Internet a organização AVTest para saber mais sobre o AV-TEST.

22.1.4

## Proteção contra malware com base na rede

A figura mostra ícones genéricos para as seguintes seções: firewalls de próxima geração, sistemas de prevenção de intrusões, controle de acesso à rede, segurança de gateway e segurança de endpoint.



Segurança do gatewayFirewalls de última geraçãoSistemas de prevenção de invasãoControle de acesso à redeSegurança de endpoint

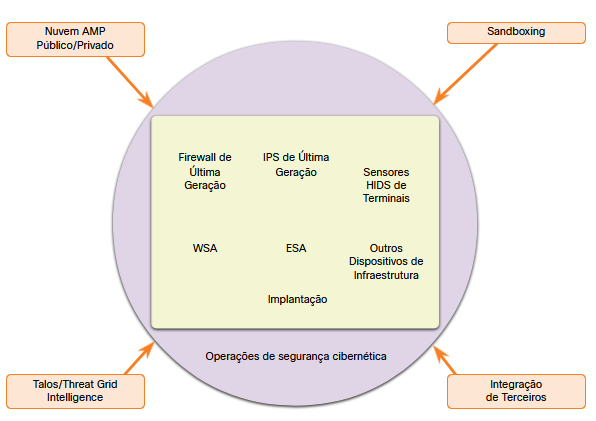
As novas arquiteturas de segurança para a rede sem fronteiras enfrentam os desafios de segurança fazendo com que os endpoints usem elementos de varredura de rede. Esses dispositivos fornecem muito mais camadas de varredura do que um único ponto de extremidade possivelmente poderia. Dispositivos de prevenção de malware baseados em rede também são capazes de compartilhar informações entre si para tomar decisões melhor informadas.

A proteção de endpoints em uma rede sem fronteiras pode ser realizada usando técnicas baseadas em rede, bem como baseadas em host, como mostrado na figura acima. Veja a seguir exemplos de dispositivos e técnicas que implementam proteções de host no nível da rede.

* **Proteção avançada contra malware (AMP)** — Isso fornece proteção de endpoint contra vírus e malware.
* **Email Security Appliance (ESA)** — Isso fornece filtragem de SPAM e e-mails potencialmente mal-intencionados antes que eles cheguem ao endpoint. Um exemplo é o Cisco ESA.
* **Web Security Appliance (WSA)** — Isso fornece filtragem de sites e lista negra para impedir que os hosts cheguem a locais perigosos na Web. O Cisco WSA fornece controle sobre como os usuários acessam a Internet e pode impor políticas de uso aceitáveis, controlar o acesso a sites e serviços específicos e verificar se há malware.
* **Controle de admissão de rede (NAC)** — Isso permite que somente sistemas autorizados e compatíveis se conectem à rede.

Essas tecnologias funcionam em conjunto umas com as outras para dar mais proteção do que as suítes baseadas em host podem fornecer, como mostrado na figura.

A figura mostra um círculo no centro rotulado como operações de segurança cibernética. Há um quadrado no meio com as seguintes palavras: firewall de próxima geração, I P S de próxima geração, sensores de ponto final H I D S, W S A, E S A e outros dispositivos de infraestrutura com a palavra implantação na parte inferior. No canto superior esquerdo está uma caixa de texto com as palavras A M P público/nuvem privada e uma seta apontando para o círculo. No canto superior direito está a caixa de texto com a palavra sandboxing e uma seta apontando para o círculo. No canto inferior direito está a caixa de texto com as palavras integração de terceiros e uma seta apontando para o círculo. No canto inferior esquerdo está uma caixa de texto com as palavras Talos/inteligência de grade de ameaças e uma seta apontando para o círculo.



# Prevenção de intrusão baseada em host

22.2.1

## Firewalls baseados em host

Firewalls pessoais baseados em host são programas de software autônomos que controlam o tráfego que entra ou sai de um computador. Aplicativos de firewall também estão disponíveis para telefones e tablets Android.

Firewalls baseados em host podem usar um conjunto de políticas predefinidas, ou perfis, para controlar pacotes que entram e saem de um computador. Eles também podem ter regras que podem ser diretamente modificadas ou criadas para controlar o acesso com base em endereços, protocolos e portas. Aplicativos de firewall baseados em host também podem ser configurados para emitir alertas aos usuários se um comportamento suspeito for detectado. Eles podem então oferecer ao usuário a capacidade de permitir que um aplicativo ofensivo seja executado ou ser impedido de ser executado no futuro.

O registro varia dependendo do aplicativo de firewall. Normalmente, inclui a data e a hora do evento, se a conexão foi permitida ou negada, informações sobre os endereços IP de origem ou destino dos pacotes e as portas de origem e destino dos segmentos encapsulados. Além disso, atividades comuns, como pesquisas de DNS e outros eventos de rotina, podem aparecer em logs de firewall baseados em host, portanto, filtragem e outras técnicas de análise são úteis para inspecionar grandes quantidades de dados de log.

Uma abordagem para a prevenção de intrusões é o uso de firewalls distribuídos. Os firewalls distribuídos combinam recursos de firewalls baseados em host com gerenciamento centralizado. A função de gerenciamento envia regras para os hosts e também pode aceitar arquivos de log dos hosts.

Independentemente de serem instalados completamente no host ou distribuídos, os firewalls baseados em host são uma camada importante de segurança de rede, juntamente com firewalls baseados em rede. Aqui estão alguns exemplos de firewalls baseados em host:

* **Firewall do Windows Defender** — Primeiro incluído no Windows XP, o Firewall do Windows (agora Firewall do Windows Defender) usa uma abordagem baseada em perfil para a funcionalidade do firewall. O acesso a redes públicas é atribuído ao perfil restritivo do firewall Público. O perfil Privado é para computadores que estão isolados da Internet por outros dispositivos de segurança, como um roteador doméstico com funcionalidade de firewall. O perfil Domínio é o terceiro perfil disponível. Ele é escolhido para conexões com uma rede confiável, como uma rede de negócios que se supõe ter uma infra-estrutura de segurança adequada. O Firewall do Windows tem funcionalidade de registo e pode ser gerido centralmente com políticas de segurança de grupo personalizadas a partir de um servidor de gestão, como o System Center 2012 Configuration Manager.
* **iptables** — Esta é uma aplicação que permite aos administradores de sistema Linux configurar regras de acesso à rede que fazem parte dos módulos Netfilter do kernel Linux.
* **nftables** — O sucessor do iptables, nftables é um aplicativo de firewall do Linux que usa uma máquina virtual simples no kernel do Linux. O código é executado dentro da máquina virtual que inspeciona pacotes de rede e implementa regras de decisão relativas à aceitação e encaminhamento de pacotes.
* **TCP Wrappers** — Este é um sistema de registro e controle de acesso baseado em regras para Linux. A filtragem de pacotes é baseada em endereços IP e serviços de rede.

22.2.2

## Detecção de intrusão baseada em host

A distinção entre detecção de intrusão baseada em host e prevenção de intrusões é desfocada. Na verdade, algumas fontes referem-se a sistemas de detecção e prevenção de intrusões baseados em host (HIPDS). Como a indústria parece favorecer o uso da sigla HIDS, vamos usá-la em nossa discussão aqui.

Um sistema de detecção de intrusões baseado em host (HIDS) foi projetado para proteger hosts contra malware conhecido e desconhecido. Um HIDS pode realizar monitoramento detalhado e relatórios sobre a configuração do sistema e a atividade do aplicativo. Ele pode fornecer análise de log, correlação de eventos, verificação de integridade, aplicação de políticas, detecção de rootkit e alertas. Um HIDS incluirá frequentemente um ponto de extremidade do servidor de gerenciamento, conforme mostrado na figura.

Um HIDS é um aplicativo de segurança abrangente que combina as funcionalidades de aplicativos antimalware com funcionalidade de firewall. Um HIDS não só detecta malware, mas também pode impedi-lo de ser executado se ele deve chegar a um host. Como o software HIDS deve ser executado diretamente no host, ele é considerado um sistema baseado em agentes.

A figura mostra uma equipe de segurança com dois PCs acima, com os logs de palavras em um e alertas abaixo do segundo e um ícone de ator de ameaça que tem um círculo com uma linha através dele sobre o ícone. Abaixo está uma rede que inclui um servidor de email e intranet que está em uma caixa colorida e um símbolo que indica um agente de detecção de intrusão baseado em host em cada servidor. Há um servidor de gerenciamento de detecção de intrusão baseado em host e setas apontando para os PCs da equipe de segurança. Existem outros dispositivos que incluem um agente de detecção de intrusões baseado em host: dois servidores, dois PCs, um laptop, um tablet e um telefone celular.

### Arquitetura de detecção de intrusões baseada em



E-mailIntranetRegistrosAlertasServidor de gerenciamento de detecção de intrusões baseado em hostEquipe de segurançaAgente de detecção de intrusões baseado em host

22.2.3

## Operação HIDS

Pode-se dizer que os sistemas de segurança baseados em host funcionam como sistemas de detecção e prevenção porque evitam ataques conhecidos e detectam ataques potenciais desconhecidos. Um HIDS usa estratégias proativas e reativas. Um HIDS pode impedir intrusões porque utiliza assinaturas para detectar malware conhecido e impedir que infecte um sistema. No entanto, esta estratégia só é boa contra ameaças conhecidas. As assinaturas não são eficazes contra ameaças novas ou de dia zero. Além disso, algumas famílias de malware exibem polimorfismo. Isso significa que variações de um tipo, ou família, de malware podem ser criadas por invasores que evitarão detecções baseadas em assinaturas alterando aspectos da assinatura de malware apenas o suficiente para que ele não seja detectado. Um conjunto adicional de estratégias é usado para detectar a possibilidade de intrusões bem-sucedidas por malware que evade a detecção de assinaturas:

* **Baseado em anomalia** - O comportamento do sistema host é comparado a um modelo de linha de base aprendido do comportamento normal. Desvios significativos da linha de base são interpretados como resultado de algum tipo de intrusão. Se uma intrusão for detectada, o HIDS poderá registrar detalhes da intrusão, enviar alertas para sistemas de gerenciamento de segurança e tomar medidas para evitar o ataque. A linha de base medida é derivada do comportamento do usuário e do sistema. Como muitas coisas além do malware podem fazer com que o comportamento do sistema mude, a detecção de anomalias pode criar muitos resultados errôneos, o que pode aumentar a carga de trabalho para o pessoal de segurança e também reduzir a credibilidade do sistema.
* **Baseado em políticas** - O comportamento normal do sistema é descrito por regras, ou a violação de regras, que são predefinidas. Violação dessas políticas resultará em ação do HIDS. O HIDS pode tentar encerrar processos de software que violaram as regras e pode registrar esses eventos e alertar o pessoal para violações. A maioria dos softwares HIDS vem com um conjunto de regras predefinidas. Com alguns sistemas, os administradores podem criar políticas personalizadas que podem ser distribuídas aos hosts a partir de um sistema central de gerenciamento de políticas.

22.2.4

## Produtos HIDS

Há uma série de produtos HIDS no mercado hoje. A maioria deles utiliza software no host e algum tipo de funcionalidade centralizada de gerenciamento de segurança que permite a integração com serviços de monitoramento de segurança de rede e inteligência contra ameaças. Exemplos são Cisco AMP, AlienVault USM, Tripwire e Segurança HIDS de código aberto (OSSEC).

O OSSEC usa um servidor de gerenciador central e agentes instalados em hosts individuais. Atualmente, os agentes estão disponíveis para plataformas Mac, Windows, Linux e Solaris. O servidor OSSEC, ou Manager, também pode receber e analisar alertas de uma variedade de dispositivos de rede e firewalls através de syslog. O OSSEC monitora os logs do sistema nos hosts e também realiza a verificação da integridade do arquivo. O OSSEC pode detectar rootkits e outros malwares e também pode ser configurado para executar scripts ou aplicativos em hosts em resposta a gatilhos de eventos.

Pesquise OSSEC na internet para saber mais.

# Segurança de aplicações

22.3.1

## Superfície de ataque

Lembre-se de que uma vulnerabilidade é uma fraqueza em um sistema ou em seu design que pode ser explorada por uma ameaça. Uma superfície de ataque é a soma total das vulnerabilidades em um determinado sistema que é acessível a um invasor. A superfície de ataque pode consistir em portas abertas em servidores ou hosts, software executado em servidores voltados para a Internet, protocolos de rede sem fio e até mesmo usuários.

A superfície de ataque continua a se expandir, como mostrado na figura. Mais dispositivos estão se conectando a redes através da Internet das Coisas (IoT) e BYOD (Traga seu próprio dispositivo). Grande parte do tráfego de rede agora flui entre dispositivos e algum local na nuvem. O uso de dispositivos móveis continua a aumentar. Todas essas tendências contribuem para uma previsão de que o tráfego IP global aumentará três vezes nos próximos cinco anos.

O Instituto SANS descreve três componentes da superfície de ataque:

* **Superfície de ataque de rede** - O ataque explora vulnerabilidades em redes. Isso pode incluir protocolos convencionais de rede com e sem fio, bem como outros protocolos sem fio usados por smartphones ou dispositivos IoT. Os ataques de rede também exploram vulnerabilidades nas camadas de rede e transporte.
* **Superfície de ataque de software** - O ataque é entregue através da exploração de vulnerabilidades em aplicativos de software baseados na Web, na nuvem ou em host.
* **Superfície de ataque humano** - O ataque explora fraquezas no comportamento do usuário. Tais ataques incluem engenharia social, comportamento malicioso por parte de dentro de confiança e erro do usuário.

A figura mostra um edifício circulado com caixas de texto em torno dele. Cada caixa de texto tem uma seta apontando para o edifício. Texto I o T Dispositivos conectados projetados para dobrar para 30 bilhões até 2020. Nuvem - até 2020, 92% das cargas de trabalho do data center serão processadas por data centers na nuvem. Mobilidade 20% do tráfego total de i p será proveniente de dispositivos móveis até 2021. O tráfego global das operações globais i p aumentará quase três vezes nos próximos cinco anos. B Y O D Gartner prevê que 70% dos profissionais realizarão trabalhos em seus próprios dispositivos inteligentes até 2018.

### Uma superfície de ataque em expansão

IoT — Dispositivos conectados projetados para dobrar para 30 bilhões até 2020.Nuvem — até 2020, 92% das cargas de trabalho do data center serão processadas por data centers na nuvem.BYOD — A Gartner prevê que 70% dos profissionais realizarão trabalhos em seus próprios dispositivos inteligentes até 2018.Operações globais - O tráfego IP global aumentará quase três vezes nos próximos 5 anos.Mobilidade — 20% do tráfego IP total será proveniente de dispositivos móveis até 2021.

22.3.2

## Lista negra e lista branca de aplicativos

Uma maneira de diminuir a superfície de ataque é limitar o acesso a ameaças potenciais criando listas de aplicativos proibidos. Isso é conhecido como lista negra.

As listas negras de aplicativos podem ditar quais aplicativos de usuário não têm permissão para serem executados em um computador. Da mesma forma, as listas brancas podem especificar quais programas podem ser executados, conforme mostrado na figura. Dessa forma, aplicativos vulneráveis conhecidos podem ser impedidos de criar vulnerabilidades em hosts de rede.

As listas brancas são criadas de acordo com uma linha de base de segurança estabelecida por uma organização. A base de referência estabelece uma quantidade de risco aceite e as componentes ambientais que contribuem para esse nível de risco. Software não incluído na lista branca pode violar a linha de base de segurança estabelecida aumentando o risco.

A figura mostra um PC com duas nuvens abaixo dele rotuladas como aplicativos de lista de permissão e aplicativos de lista de bloqueio. Há uma seta saindo da nuvem de aplicativos da lista de permissões apontando para o pc e uma caixa de texto que indica permitir somente. Os aplicativos de lista de bloqueio têm uma seta apontando para o pc e uma caixa de texto que diz impedir apenas ao lado da seta.

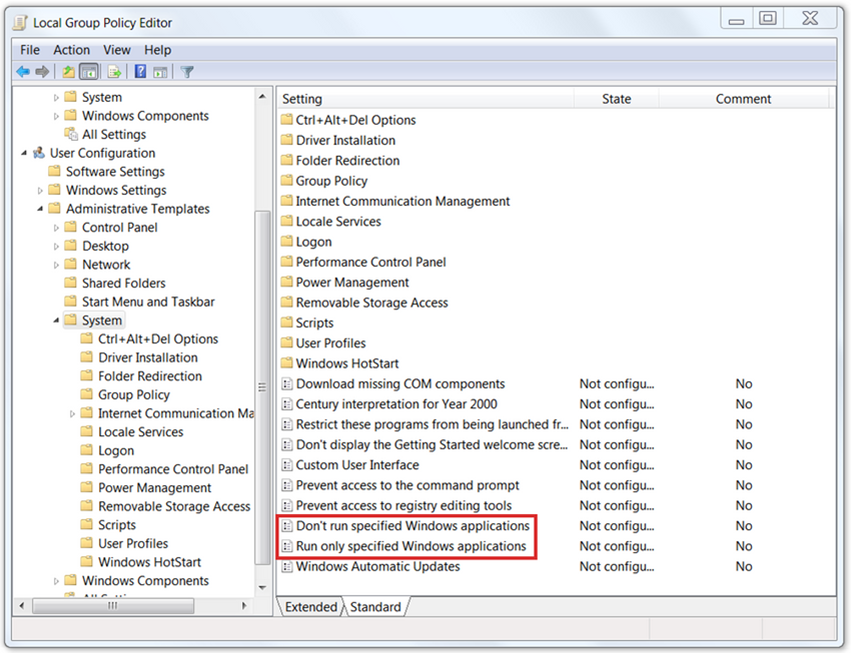
### Lista de bloqueio de aplicativos e lista de permissões

Permitir aplicativos da listaPermitir SomentePrevenir SomenteAplicativos de lista de bloqueio

A figura mostra as configurações da lista negra e da lista branca do Editor de Diretiva de Grupo Local do Windows.

Os sites também podem ser incluídos na lista branca e na lista negra. Essas listas negras podem ser criadas manualmente ou podem ser obtidas de vários serviços de segurança. As listas negras podem ser continuamente atualizadas pelos serviços de segurança e distribuídas para firewalls e outros sistemas de segurança que as utilizam. O sistema de gerenciamento de segurança Firepower da Cisco é um exemplo de um sistema que pode acessar o serviço de inteligência de segurança Cisco Talos para obter listas negras. Essas listas negras podem então ser distribuídas para dispositivos de segurança dentro de uma rede corporativa.

Pesquise na internet The Spamhaus Project, que é um exemplo de um serviço gratuito de lista negra.



22.3.3

## Sandboxing baseado em sistema

Sandboxing é uma técnica que permite que arquivos suspeitos sejam executados e analisados em um ambiente seguro. As sandboxes de análise automatizada de malware oferecem ferramentas que analisam o comportamento do malware. Essas ferramentas observam os efeitos da execução de malware desconhecido para que os recursos do comportamento de malware possam ser determinados e usados para criar defesas contra ele.

Como mencionado anteriormente, o malware polimórfico muda com freqüência e o novo malware aparece regularmente. O malware entrará na rede apesar dos sistemas de segurança baseados em host e perímetro mais robustos. HIDS e outros sistemas de detecção podem criar alertas sobre suspeita de malware que pode ter entrado na rede e executado em um host. Sistemas como o Cisco AMP podem rastrear a trajetória de um arquivo através da rede e podem “reverter” eventos de rede para obter uma cópia do arquivo baixado. Esse arquivo pode ser executado em uma área restrita, como o Cisco Threat Grid Glivebox, e as atividades do arquivo documentado pelo sistema. Essas informações podem então ser usadas para criar assinaturas para impedir que o arquivo entre na rede novamente. As informações também podem ser usadas para criar regras de detecção e reproduções automatizadas que identificam outros sistemas que foram infectados.

Cuckoo Sandbox é um sandbox popular sistema de análise de malware livre. Ele pode ser executado localmente e ter amostras de malware enviadas a ele para análise. Existem várias outras sandboxes públicas online. Esses serviços permitem que amostras de malware sejam carregadas para análise. Alguns desses serviços são VirusTotal, Joe Sandbox e CrowdStrike Falcon Sandbox.

Uma ferramenta online interessante é ANY.RUN, que é mostrado na figura. Ele oferece a capacidade de carregar uma amostra de malware para análise como qualquer sandbox online. No entanto, ele oferece uma funcionalidade de relatórios interativos muito rica que está cheia de detalhes sobre o exemplo de malware. ANY.RUN executa o malware e captura uma série de capturas de tela do malware se ele tiver elementos interativos que são exibidos na tela do computador sandbox. Você pode exibir amostras públicas que foram enviadas por usuários ANY.RUN para investigar informações sobre malware recém-descoberto ou malware que está circulando atualmente na Internet. Os relatórios incluem a atividade de rede e internet do malware, incluindo solicitações HTTP e consultas DNS. Os arquivos que são executados como parte do processo de malware são mostrados e classificados como ameaça. Os detalhes estão disponíveis para os arquivos, incluindo vários valores de hash, exibições hexadecimais e ASCII do conteúdo do arquivo e as alterações do sistema feitas pelos arquivos. Além disso, identificar indicadores de comprometimento, como hashes de arquivo de malware, solicitações DNS e as conexões IP feitas pelo malware também são mostrados. Finalmente, as táticas adotadas pelo malware são mapeadas para a Matriz MITRE ATT&CK com cada tática vinculada aos detalhes no site MITRE.



22.3.4

## Vídeo - Usando uma sandbox para iniciar malware

Reproduza o vídeo para ver uma demonstração do uso do ambiente sandbox para iniciar e analisar um ataque de malware.

# Resumo de proteção de endpoint

22.4.1

## O que aprendi neste módulo?

**Proteção Antimalware**

Podemos definir endpoints como hosts na rede que pode acessar ou ser acessado por outros hosts na rede. Isso obviamente inclui computadores e servidores. Com o rápido crescimento da Internet das Coisas (IoT), outros tipos de dispositivos são agora endpoints na rede. Cada ponto de extremidade é uma forma potencial de software malicioso ter acesso a uma rede. Nem todos os endpoints estão dentro de uma rede. Muitos endpoints se conectam a redes remotamente através de VPN. O perímetro da rede está sempre se expandindo. Vários dispositivos de segurança de rede são necessários para proteger o perímetro da rede contra acesso externo. No entanto, muitos ataques também se originam de dentro da rede. Portanto, proteger uma LAN interna é quase tão importante quanto proteger o perímetro externo da rede. Depois que um host interno é infiltrado, ele pode se tornar um ponto de partida para um invasor obter acesso a dispositivos críticos do sistema. Há dois elementos de LAN internos para proteger: endpoints e infra-estrutura de rede.

O Software Antivírus/Antimalware é instalado em um host para detectar e mitigar vírus e malware. Ele faz isso usando três abordagens diferentes, baseadas em assinaturas (usando várias características de arquivos de malware conhecidos), heurística (usando recursos gerais compartilhados por vários tipos de malware) e baseado em comportamento (usando uma análise de comportamento suspeito). Muitos programas antivírus são capazes de fornecer proteção em tempo real analisando dados conforme eles são usados pelo endpoint. Um Firewall baseado em host restringe as conexões de entrada e saída a conexões iniciadas somente por esse host. Alguns softwares de firewall também podem impedir que um host se infecte e impedir que hosts infectados espalhem malware para outros hosts. A maioria dos softwares de segurança baseados em host inclui funcionalidade de registro que é essencial para operações de segurança cibernética. Dispositivos de prevenção de malware baseados em rede também são capazes de compartilhar informações entre si para tomar decisões melhor informadas. A proteção de endpoints em uma rede sem fronteiras pode ser realizada usando técnicas baseadas em rede, bem como baseadas em host.

**Prevenção de intrusão baseada em host**

Firewalls baseados em host podem usar um conjunto de políticas predefinidas, ou perfis, para controlar pacotes que entram e saem de um computador. Eles também podem ter regras que podem ser diretamente modificadas ou criadas para controlar o acesso com base em endereços, protocolos e portas. Eles também podem ser configurados para emitir alertas se um comportamento suspeito for detectado. O registro varia dependendo do aplicativo de firewall. Normalmente, inclui a data e a hora do evento, se a conexão foi permitida ou negada, informações sobre os endereços IP de origem ou destino dos pacotes e as portas de origem e destino dos segmentos encapsulados. Firewalls distribuídos também podem ser usados. Eles combinam recursos de firewalls baseados em host com gerenciamento centralizado. Alguns exemplos de firewalls baseados em host incluem Firewall do Windows Defender, iptables, nftables e TCP Wrappers. Um sistema de detecção de intrusões baseado em host (HIDS) protege os hosts contra malware conhecido e desconhecido. Um HIDS pode realizar monitoramento e relatórios detalhados sobre a configuração do sistema e a atividade do aplicativo, análise de log, correlação de eventos, verificação de integridade, aplicação de políticas, detecção de rootkit e alertas. Um HIDS incluirá frequentemente um endpoint de servidor de gerenciamento. Como o software HIDS deve ser executado diretamente no host, ele é considerado um sistema baseado em agentes. Um HIDS usa estratégias proativas e reativas. Um HIDS pode impedir intrusões porque utiliza assinaturas para detectar malware conhecido e impedir que infecte um sistema. As assinaturas não são eficazes contra ameaças novas ou de dia zero. Além disso, algumas famílias de malware exibem polimorfismo. Estratégias adicionais para detectar a possibilidade de sucesso incluem detecção baseada em anomalias e detecção baseada em políticas.

**Segurança de aplicações**

Uma superfície de ataque é a soma total das vulnerabilidades em um determinado sistema que é acessível a um invasor. Pode consistir em portas abertas em servidores ou hosts, software que está sendo executado em servidores voltados para a Internet, protocolos de rede sem fio, dispositivos remotos e até mesmo usuários. A superfície de ataque continua a expandir-se. Mais dispositivos estão se conectando a redes através da Internet das Coisas (IoT) e BYOD (Traga seu próprio aparelho). O Instituto SANS descreve três componentes da superfície de ataque: superfície de ataque de rede, superfície de ataque de software e superfície de ataque humano. Uma maneira de diminuir a superfície de ataque é limitar o acesso a ameaças potenciais criando listas de aplicativos proibidos. Isso é conhecido como lista negra. As listas negras de aplicativos podem ditar quais aplicativos de usuário não têm permissão para serem executados em um computador. Da mesma forma, as listas brancas podem especificar quais programas podem ser executados. As listas brancas são criadas de acordo com uma linha de base de segurança estabelecida por uma organização. As listas negras podem ser criadas manualmente ou podem ser obtidas a partir de vários serviços de segurança. Sandboxing é uma técnica que permite que arquivos suspeitos sejam executados e analisados em um ambiente seguro. As sandboxes de análise automatizada de malware oferecem ferramentas que analisam o comportamento do malware. Essas ferramentas observam os efeitos da execução de malware desconhecido para que os recursos do comportamento de malware possam ser determinados e usados para criar defesas contra ele. O malware polimórfico muda com frequência e o novo malware aparece regularmente. O malware entrará na rede apesar dos sistemas de segurança baseados em host e perímetro mais robustos. HIDS e outros sistemas de detecção podem criar alertas sobre suspeita de malware que pode ter entrado na rede e executado em um host.

# Introdução

23.0.1

## Por que devo cursar este módulo?

Quanto dinheiro uma organização deve gastar em segurança de rede e operações cibernéticas? Como uma organização sabe quanto esforço e recursos deve colocar para manter a rede e os dados seguros? Essas perguntas podem ser respondidas através da avaliação de risco e vulnerabilidade. Analistas de segurança cibernética e especialistas em segurança usam uma variedade de ferramentas para realizar avaliações de vulnerabilidade. A criação de perfis de rede e dispositivo fornece uma linha de base que serve como ponto de referência para identificar desvios em relação às operações normais. Da mesma forma, a criação de perfil do servidor é usada para estabelecer o estado operacional aceito dos servidores. As organizações usam o Common Vulnerability Scoring System (CVSS) para ponderar os riscos de uma vulnerabilidade usando uma variedade de métricas. Em seguida, as organizações aplicam técnicas de gerenciamento de risco para selecionar e especificar seus controles de segurança. As organizações usam um Sistema de Gerenciamento de Segurança da Informação (ISMS) para identificar, analisar e lidar com os riscos de segurança das informações. Este módulo aborda detalhes da criação de perfis de rede e servidor, CVSS, técnicas de gerenciamento de risco e ISMS.

23.0.2

## O que vou aprender neste módulo?

**Título do módulo:** Avaliação de vulnerabilidade de endpoint

**Objetivo do módulo:** Explicar como as vulnerabilidades do endpoint são avaliadas e gerenciadas.

| **Título do Tópico** | **Objetivo do Tópico** |
| --- | --- |
| Perfil de rede e servidor | Explicar o valor do perfil de rede e servidor. |
| Sistema de pontuação de vulnerabilidade comum (CVSS) | Explicar como os relatórios de CVSS são usados para descrever as vulnerabilidades de segurança. |
| Gerenciamento seguro de dispositivos | Explicar como as técnicas de gerenciamento de dispositivo seguro são usadas para proteger dados e ativos. |
| Sistemas de Gestão de Segurança da Informação | Explicar como os sistemas de gerenciamento de segurança da informação são usados para proteger os ativos. |

# Perfil de rede e servidor

23.1.1

## Perfil de rede

Para detectar incidentes de segurança graves, é importante compreender, caracterizar e analisar informações sobre o funcionamento normal da rede. Todas as redes, servidores e hosts exibem um comportamento típico para um determinado ponto no tempo. A criação de perfis de rede e dispositivo pode fornecer uma linha de base estatística que serve como ponto de referência. Desvios inexplicáveis em relação à linha de base podem indicar um compromisso.

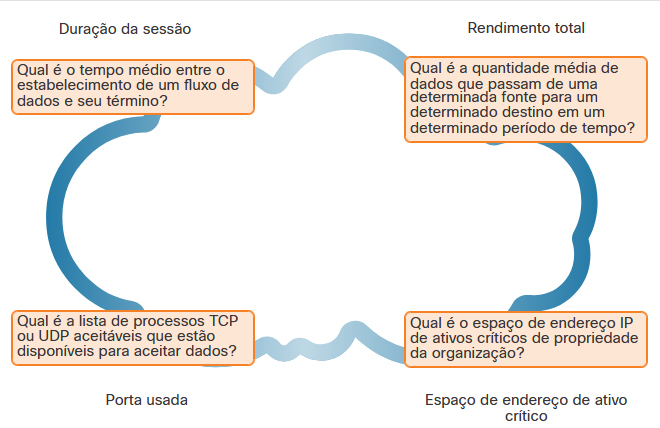
Deve-se ter cuidado ao capturar dados de linha de base para que todas as operações normais de rede sejam incluídas na linha de base. Além disso, é importante que a linha de base seja atual. Não deve incluir dados de desempenho da rede que não façam mais parte do funcionamento normal. Por exemplo, aumentos na utilização da rede durante operações periódicas de backup do servidor fazem parte do funcionamento normal da rede e devem fazer parte dos dados da linha de base. No entanto, a medição do tráfego que corresponde ao acesso externo a um servidor interno que foi movido para a nuvem não seria. Um meio de capturar apenas o período certo para medição de linha de base é conhecido como detecção de anomalias de janela deslizante. Ele define uma janela que é mais representativa da operação de rede e exclui dados que estão desatualizados. Esse processo continua com medições repetidas da linha de base para garantir que as estatísticas de medição da linha de base retratem a operação da rede com a máxima precisão.

O aumento da utilização de links WAN em momentos incomuns pode indicar uma violação de rede e uma extracção de dados. Os hosts que começam a acessar servidores obscuros da Internet, resolvem domínios obtidos por meio de DNS dinâmico ou usam protocolos ou serviços que não são necessários para o usuário do sistema também podem indicar comprometimento. Desvios no comportamento da rede são difíceis de detectar se o comportamento normal não é conhecido.

Ferramentas como NetFlow e Wireshark podem ser usadas para caracterizar características normais de tráfego de rede. Como as organizações podem fazer demandas diferentes em suas redes dependendo da hora do dia ou do dia do ano, a linha de base da rede deve ser realizada durante um período prolongado. A figura exibe algumas perguntas a serem feitas ao estabelecer uma linha de base de rede.

A imagem é uma nuvem. No canto superior esquerdo da imagem está uma caixa de texto conectada à nuvem chamada Duração da sessão. A caixa de texto contém a pergunta: Qual é o tempo médio entre o estabelecimento de um fluxo de dados e seu término? No canto superior direito da imagem está uma caixa de texto conectada à nuvem rotulada como Taxa de transferência total. A caixa de texto contém a pergunta: Qual é a quantidade média de dados que passam de uma determinada fonte para um determinado destino em um determinado período de tempo? No canto inferior esquerdo da imagem está uma caixa de texto conectada à nuvem rotulada como Porta usada. A caixa de texto contém a pergunta: Qual é a lista de processos TCP ou UDP aceitáveis que estão disponíveis para aceitar dados? No canto inferior direito da imagem, há uma caixa de texto conectada à nuvem rotulada Espaço de endereço de ativo crítico. A caixa de texto contém a pergunta: Qual é o espaço de endereço IP dos ativos críticos de propriedade da organização?

### Elementos de um Perfil de Rede



Qual é a quantidade média de dados que passam de uma determinada fonte para um determinado destino em um determinado período de tempo?Qual é o espaço de endereço IP de ativos críticos de propriedade da organização?Qual é o tempo médio entre o estabelecimento de um fluxo de dados e seu término?Duração da sessãoQual é a lista de processos TCP ou UDP aceitáveis que estão disponíveis para aceitar dados?Rendimento totalPorta usadaEspaço de endereço de ativo crítico

A tabela lista elementos importantes do perfil de rede.

| **Elemento Perfil de Rede** | **Descrição** |
| --- | --- |
| **Duração da sessão** | Este é o tempo entre o estabelecimento de um fluxo de dados e seu término. |
| **Rendimento total** | Esta é a quantidade de dados que passam de uma determinada fonte para um determinado destino em um determinado período de tempo. |
| **Portas usadas** | Esta é uma lista de processos TCP ou UDP que estão disponíveis para aceitar dados. |
| **Espaço de endereço de ativo crítico** | Estes são os endereços IP ou a localização lógica de sistemas ou dados essenciais. |

Além disso, um perfil dos tipos de tráfego que normalmente entram e saem da rede é uma ferramenta importante para compreender o comportamento da rede. O malware pode usar portas incomuns que podem não ser vistas normalmente durante a operação normal da rede. O tráfego de host para host é outra métrica importante. A maioria dos clientes de rede se comunica diretamente com servidores, portanto, um aumento do tráfego entre clientes pode indicar que o malware está se espalhando lateralmente pela rede.

Finalmente, alterações no comportamento do usuário, conforme revelado pelo AAA, logs do servidor ou um sistema de criação de perfil do usuário, como o Cisco Identity Services Engine (ISE), é outro indicador valioso. Saber como os usuários individuais normalmente usam a rede leva à detecção de potencial comprometimento das contas de usuário. Um usuário que de repente começa a fazer login na rede em momentos estranhos a partir de um local remoto deve gerar alarmes se esse comportamento for um desvio de uma norma conhecida.

23.1.2

## Perfil de servidor

A definição de perfil do servidor é usada para estabelecer o estado operacional aceito dos servidores. Um perfil de servidor é uma linha de base de segurança para um determinado servidor. Estabelece os parâmetros de rede, usuário e aplicativo que são aceitos para um servidor específico.

Para estabelecer um perfil de servidor, é importante entender a função que um servidor se destina a executar em uma rede. A partir daí, vários parâmetros operacionais e de uso podem ser definidos e documentados.

A tabela lista elementos de um perfil de servidor.

| **Elemento de Perfil de Servidor** | **Descrição** |
| --- | --- |
| **Portas de escuta** | Esses são os daemons e portas TCP e UDP que normalmente podem ser abertos no servidor. |
| **Usuários e contas logadas** | Estes são os parâmetros que definem o acesso e o comportamento do usuário. |
| **Contas de serviço** | Estas são as definições do tipo de serviço que um aplicativo tem permissão para executar. |
| **Ambiente de software** | Estas são as tarefas, processos e aplicativos que podem ser executados no servidor. |

23.1.3

## Detecção de anomalias de rede

O comportamento da rede é descrito por uma grande quantidade de dados diversos, como os recursos do fluxo de pacotes, os recursos dos próprios pacotes e a telemetria de várias fontes. Uma abordagem para a detecção de ataques de rede é a análise desses dados diversos e não estruturados usando técnicas de análise de Big Data. Isso é conhecido como análise de comportamento de rede (NBA).

Isto implica a utilização de técnicas sofisticadas de aprendizagem estatística e de máquina para comparar as linhas de base de desempenho normais com o desempenho da rede num determinado momento. Desvios significativos podem ser indicadores de compromisso. Além disso, o comportamento da rede pode ser analisado quanto a comportamentos de rede conhecidos que indicam comprometimento.

A detecção de anomalias pode reconhecer o tráfego de rede causado pela atividade de worm que exibe o comportamento de varredura. A detecção de anomalias também pode identificar hosts infectados na rede que estão verificando outros hosts vulneráveis.

A figura ilustra uma versão simplificada de um algoritmo projetado para detectar uma condição incomum nos roteadores de fronteira de uma empresa.

A figura mostra uma caixa de texto rotulada nos roteadores de borda a cada x min: e uma seta para a próxima caixa de texto chamada contagem flui com amostragem de 1/6 durante z seg com uma seta fluindo para baixo para um símbolo de decisão com as palavras se # de fluxos > N. A seta sim aponta para uma caixa chamada Alarme! A seta agora aponta para uma caixa rotulada final. O alarme! Caixa tem uma seta apontando para a mesma caixa rotulada final.

Contagem de fluxos com Amostragem 1/Y durante Z segSe # de fluxos > NSimEm Roteadores de fronteira, a cada X min:finalizarAlarme!Não

Por exemplo, o analista de segurança cibernética poderia fornecer os seguintes valores:

* X = 5
* Y = 100
* Z = 30
* N = 500

Agora, o algoritmo pode ser interpretado como: a cada 5 minutos, obter uma amostragem de 1/100 dos fluxos durante o segundo 30. Se o número de fluxos for maior que 500, gere um alarme. Se o número de fluxos for inferior a 500, não faça nada. Este é um exemplo simples de usar um perfil de tráfego para identificar o potencial de perda de dados.

Além de abordagens estatísticas e comportamentais para detecção de anomalias é a detecção de anomalias baseada em regras. A detecção baseada em regras analisa pacotes decodificados para ataques com base em padrões predefinidos.

23.1.4

## Teste de vulnerabilidade de rede

A maioria das organizações conecta-se às redes públicas de alguma forma devido à necessidade de acessar a internet. Essas organizações também devem fornecer serviços voltados para a internet de vários tipos ao público. Devido ao grande número de potenciais vulnerabilidades e ao fato de que novas vulnerabilidades podem ser criadas dentro de uma rede da organização e seus serviços voltados para a Internet, testes periódicos de segurança são essenciais.

A tabela lista vários tipos de testes que podem ser realizados.

| **Termo** | **Descrição** |
| --- | --- |
| **Análise de risco** | * Esta é uma disciplina na qual os analistas avaliam o risco representado pelas vulnerabilidades a uma organização específica. * Uma análise de risco inclui a avaliação da probabilidade de ataques, identifica tipos de possíveis agentes de ameaça e avalia o impacto de explorações bem-sucedidas na organização. |
| **Avaliação de vulnerabilidade** | * Este teste emprega software para verificar servidores voltados para a Internet e redes internas em busca de vários tipos de vulnerabilidades. * Essas vulnerabilidades incluem infecções desconhecidas, fraquezas nos serviços de banco de dados voltados para a Web, patches de software ausentes, portas de escuta desnecessárias etc. * As ferramentas para avaliação de vulnerabilidades incluem a plataforma OpenVAS de código aberto, o Microsoft Baseline Security Analyzer, o Nessus, a Qualys e os serviços FireEye Mandiant. * A avaliação de vulnerabilidades inclui, mas vai além, a varredura de portas. |
| **Teste de penetração** | * Esse tipo de teste usa ataques simulados autorizados para testar a força da segurança da rede. * O pessoal interno com experiência em hackers ou hackers éticos profissionais identifica ativos que podem ser alvo de agentes de ameaças. * Uma série de explorações é usada para testar a segurança desses ativos. * Ferramentas de software de exploração simuladas são frequentemente usadas. * O teste de penetração não só verifica se existem vulnerabilidades, como também explora essas vulnerabilidades para determinar o impacto potencial de uma exploração bem-sucedida. * Um teste de penetração individual é frequentemente conhecido como teste de caneta. * Metasploit é uma ferramenta usada em testes de penetração. * CORE Impact oferece software e serviços de teste de penetração. |

A tabela lista exemplos de atividades e ferramentas que são usadas em testes de vulnerabilidade.

| **Atividade de** | **Descrição** | **Ferramentas** |
| --- | --- | --- |
| **Análise de risco** | Indivíduos realizam uma análise abrangente dos impactos dos ataques nos ativos principais da empresa e no funcionamento | Consultores internos ou externos, quadros de gestão de riscos |
| **Avaliação de vulnerabilidade** | Gerenciamento de patches, varreduras de host, varredura de portas, outras verificações de vulnerabilidade e serviços | OpenVAS, Analisador de Linha de Base da Microsoft, Nessus, Qualys, Nmap |
| **Teste de penetração** | Uso de técnicas e ferramentas de hacking para penetrar nas defesas da rede e identificar a profundidade de penetração potencial | Metasploit, CORE Impact, hackers éticos |

# Sistema de pontuação de vulnerabilidade comum (CVSS)

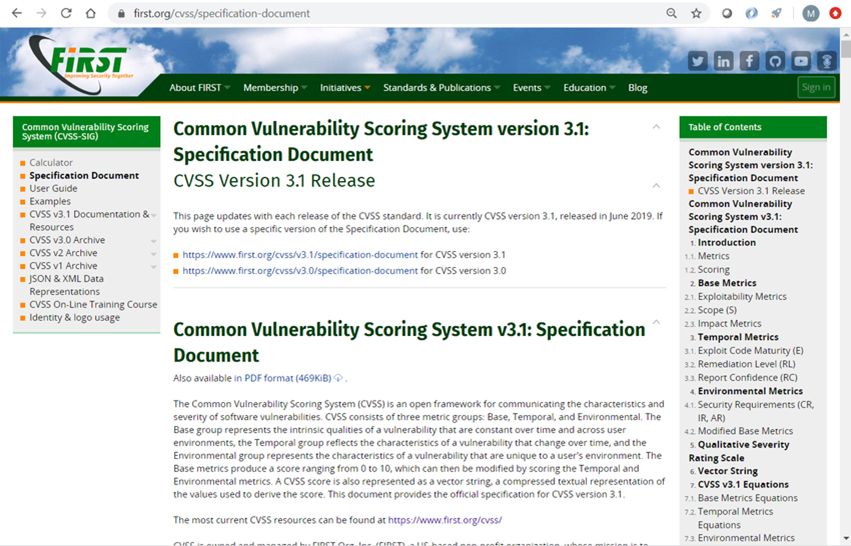
23.2.1

## Visão geral do CVSS

O Common Vulnerability Scoring System (CVSS) é uma ferramenta de avaliação de risco projetada para transmitir os atributos comuns e a gravidade das vulnerabilidades em sistemas de hardware e software de computador. A terceira revisão, CVSS 3.0, é uma estrutura aberta e neutra do fornecedor, padrão do setor, para ponderar os riscos de uma vulnerabilidade usando uma variedade de métricas. Esses pesos combinam-se para fornecer uma pontuação do risco inerente a uma vulnerabilidade. A pontuação numérica pode ser usada para determinar a urgência da vulnerabilidade e a prioridade de abordá-la. Os benefícios do CVSS podem ser resumidos da seguinte forma:

* Ele fornece pontuações padronizadas de vulnerabilidade que devem ser significativas em todas as organizações.
* Ele fornece uma estrutura aberta com o significado de cada métrica abertamente disponível para todos os usuários.
* Ele ajuda a priorizar o risco de uma forma que seja significativa para organizações individuais.

O Fórum de Equipes de Resposta a Incidentes e Segurança (FIRST) foi designado como guardião do CVSS para promover sua adoção globalmente. O padrão Versão 3 foi desenvolvido com contribuições da Cisco e de outros parceiros do setor. A versão 3.1 foi lançada em junho de 2019. A figura exibe a página de especificação do CVSS no site FIRST.



23.2.2

## Grupos métricos CVSS

Antes de realizar uma avaliação do CVSS, é importante conhecer os termos fundamentais utilizados no instrumento de avaliação.

Muitas das métricas abordam o papel do que o CVSS chama de autoridade. Uma autoridade é uma entidade de computador, como um banco de dados, sistema operacional ou caixa de proteção virtual, que concede e gerencia acesso e privilégios aos usuários.

A imagem exibe os Grupos Métricos do CVSS. Há três caixas mostradas lado a lado. A primeira caixa, à esquerda, é intitulada Grupo de Métricas Base. Nesta caixa estão duas colunas: Métricas de Exploração e Métricas de Impacto. Na coluna Explorabilidade há quatro itens: vetor de ataque, complexidade de ataque, privilégios necessários e interação do usuário. Na coluna Impacto estão três itens: impacto na confidencialidade, impacto na integridade e impacto na disponibilidade. Abrangendo ambas as colunas na parte inferior é Escopo. A segunda caixa, no meio, é intitulada Grupo Métrico Temporal. Esta caixa contém três itens: maturidade do código de exploração, nível de correção e confiança do relatório. A terceira caixa, à direita, são quatro caixas: Métricas Base Modificadas, requisito de confidencialidade, requisito de integridade e requisito de disponibilidade.

### Grupos métricos CVSS



Como mostrado na figura, o CVSS usa três grupos de métricas para avaliar a vulnerabilidade.

**Grupo de métricas base**

Isso representa as características de uma vulnerabilidade que são constantes ao longo do tempo e em contextos. Ele tem duas classes de métricas:

* **Explorabilidade** \ - Esses são recursos da exploração, como vetor, complexidade e interação do usuário exigidas pela exploração.
* **Métricas de impacto** - Os impactos da exploração estão enraizados na tríade de confidencialidade, integridade e disponibilidade da CIA.

**Grupo métrico temporal**

Isso mede as características de uma vulnerabilidade que pode mudar ao longo do tempo, mas não em ambientes de usuário. Ao longo do tempo, a gravidade de uma vulnerabilidade mudará à medida que for detectada e serão desenvolvidas medidas para combatê-la. A gravidade de uma nova vulnerabilidade pode ser alta, mas diminuirá à medida que patches, assinaturas e outras contramedidas forem desenvolvidas.

**Grupo métrico ambiental**

Isso mede os aspectos de uma vulnerabilidade que estão enraizados no ambiente de uma organização específica. Essas métricas ajudam a classificar as consequências dentro de uma organização e permitem o ajuste de métricas menos relevantes para o que uma organização faz.

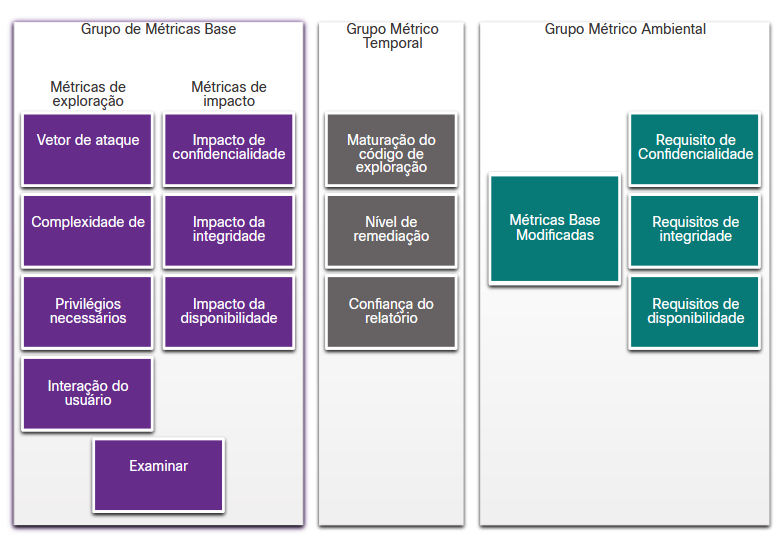
23.2.3

## Grupo Métrico Base CVSS

A figura destaca o Grupo de Métricas Base.

A figura tem a mesma figura de grupos métricos CVSS como antes com o grupo métrico base destacado.

### Grupos métricos CVSS



Vetor de ataqueImpacto de confidencialidadeComplexidade deImpacto da integridadePrivilégios necessáriosImpacto da disponibilidadeInteração do usuárioExaminarGrupo de Métricas BaseGrupo Métrico AmbientalGrupo Métrico TemporalMétricas de exploraçãoMétricas de impactoMaturação do código de exploraçãoNível de remediaçãoConfiança do relatórioRequisito de ConfidencialidadeMétricas Base ModificadasRequisitos de integridadeRequisitos de disponibilidade

A tabela lista os critérios para as métricas de Explorabilidade do Grupo de Métricas Base.

| **Critérios** | **Descrição** |
| --- | --- |
| **Vetor de ataque** | Esta é uma métrica que reflete a proximidade do ator da ameaça com o componente vulnerável. Quanto mais remoto for o ator de ameaça para o componente, maior será a gravidade. Os agentes de ameaças próximos à sua rede ou dentro da sua rede são mais fáceis de detectar e mitigar. |
| **A complexidade do ataque** | Esta é uma métrica que expressa o número de componentes, software, hardware ou redes, que estão além do controle do invasor e que devem estar presentes para que uma vulnerabilidade seja explorada com êxito. |
| **Privilégios necessários** | Esta é uma métrica que captura o nível de acesso necessário para uma exploração bem-sucedida da vulnerabilidade. |
| **Interação do usuário** | Esta métrica expressa a presença ou ausência do requisito de interação do usuário para que uma exploração seja bem-sucedida. |
| **Escopo** | Esta métrica expressa se várias autoridades devem estar envolvidas em uma exploração. Isto é expresso como se a autoridade inicial mudasse para uma segunda autoridade durante a exploração. |

As métricas de Impacto do Grupo Métrico Base aumentam com o grau ou conseqüência da perda devido ao componente afetado. A tabela lista os componentes de métrica de impacto.

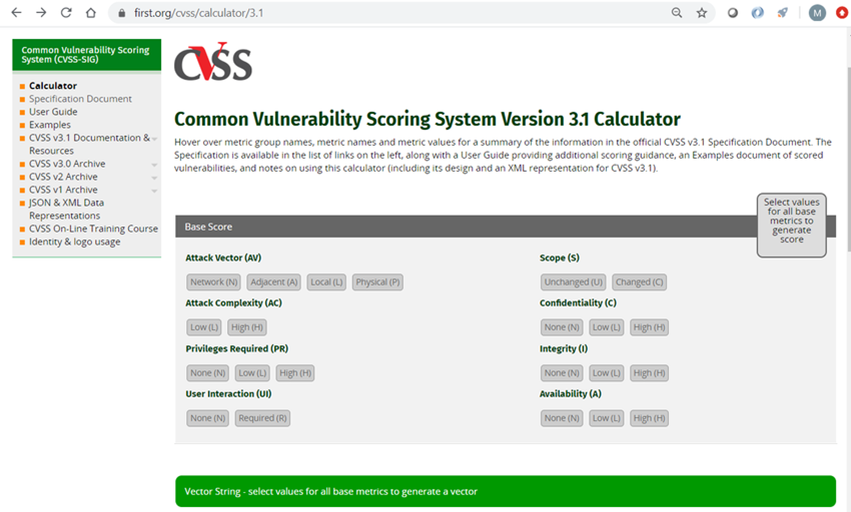
| **Termo** | **Descrição** |
| --- | --- |
| **Impacto de Confidencialidade** | Esta é uma métrica que mede o impacto na confidencialidade devido a uma vulnerabilidade explorada com sucesso. Confidencialidade refere-se à limitação do acesso apenas a usuários autorizados. |
| **Impacto da integridade** | Esta é uma métrica que mede o impacto na integridade devido a uma vulnerabilidade explorada com sucesso. Integridade refere-se à confiabilidade e autenticidade das informações. |
| **Impacto da disponibilidade** | Esta é uma métrica que mede o impacto na disponibilidade devido a uma vulnerabilidade explorada com sucesso. Disponibilidade refere-se à acessibilidade de informações e recursos de rede. Os ataques que consomem largura de banda da rede, ciclos de processador ou espaço em disco afetam a disponibilidade. |

23.2.4

## O Processo CVSS

O CVSS Base Metrics Group foi projetado como uma forma de avaliar vulnerabilidades de segurança encontradas em sistemas de software e hardware. Ele descreve a gravidade de uma vulnerabilidade com base nas características de uma exploração bem-sucedida da vulnerabilidade. Os outros grupos de métricas modificam a pontuação de gravidade base, contabilizando como a classificação de gravidade base é afetada por fatores de tempo e ambientais.

O processo CVSS usa uma ferramenta chamada Calculadora CVSS v3.1, mostrada na figura.

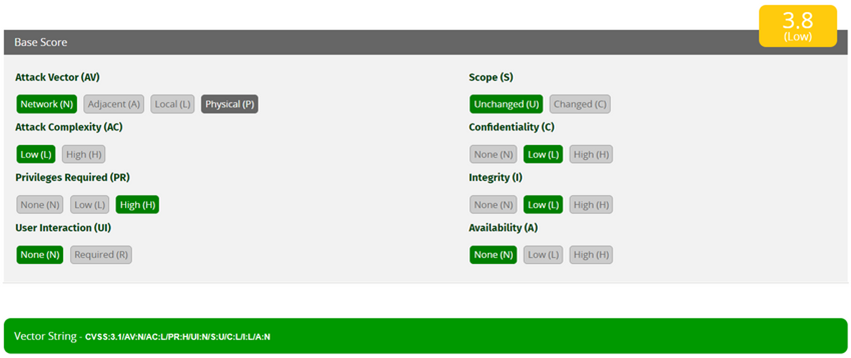


A calculadora é como um questionário no qual são feitas escolhas que descrevem a vulnerabilidade para cada grupo de métricas. Depois que todas as escolhas são feitas, uma pontuação é gerada. O texto pop-up que explica cada métrica e valor métrico é exibido passando o mouse sobre cada um. As opções são feitas escolhendo um dos valores para a métrica. Apenas uma escolha pode ser feita por métrica.

A calculadora CVSS pode ser acessada na parte CVSS do site FIRST.

Um guia detalhado do usuário que define critérios métricos, exemplos de avaliações de vulnerabilidades comuns e a relação de valores métricos com a pontuação final está disponível para dar suporte ao processo.

Após a conclusão do grupo Métrica Base, a classificação de gravidade numérica é exibida, conforme mostrado na figura.



Uma string vetorial também é criada que resume as escolhas feitas. Se outros grupos métricos forem concluídos, esses valores serão anexados à string vetorial. A string consiste na (s) inicial (s) para a métrica e um valor abreviado para o valor métrico selecionado separado por dois-pontos. Os pares de valor métrico são separados por barras. As strings vetoriais permitem que os resultados da avaliação sejam facilmente compartilhados e comparados.

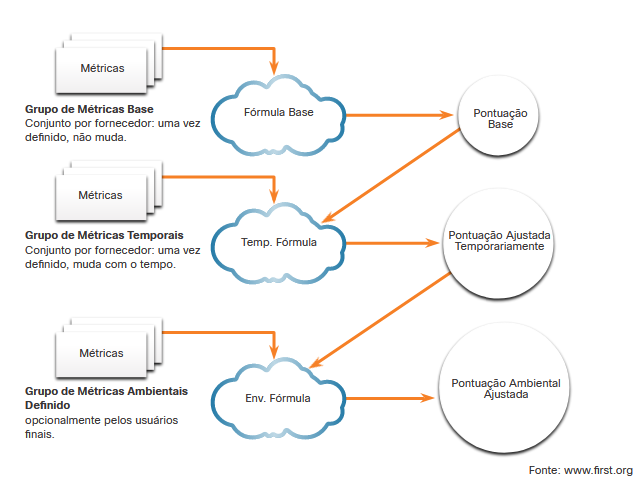
A tabela lista a chave para o grupo Métrica Base.

| **Nome da Métrica** | **Iniciais** | **Valores Possíveis** | **Valores** |
| --- | --- | --- | --- |
| **Vetor de ataque** | AV | [N, A, L, P] | N = Network  A = Adjacente  L = Local  P = Físico |
| **Complexidade de Ataque** | AC | [L, H] | L = Baixo  H = Alto |
| **Privilégios necessários** | PR | [N, L, H] | N = Nenhum  L = Baixo  H = Alto |
| **Interação do usuário** | UI | [N, R] | N = Nenhum  R = Requerido |
| **Escopo** | S | [U, C] | U = Inalterado  C = Modificado |
| **Impacto de Confidencialidade** | C | [H, L, N] | H = Alto  L = Baixo  N = Nenhum |
| **Impacto da integridade** | S | [H, L, N] | H = Alto  L = Baixo  N = Nenhum |
| **Impacto da disponibilidade** | R | [H, L, N] | H = Alto  L = Baixo  N = Nenhum |

Os valores para a cadeia de classificação de gravidade numérica **CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:N** são listados na tabela.

| **Nome da Métrica** | **Valores** |
| --- | --- |
| Vetor de ataque, AV | Captura de dados |
| Complexidade de ataque, AC | Baixa |
| Privilégios Obrigatórios, PR | Alto |
| Interação do usuário, IU | Nenhum |
| Âmbito, S | Inalterado |
| Confidentiality Impact, C | Baixa |
| Impacto da Integridade, I | Baixa |
| Impacto na disponibilidade, A | Nenhum |

Para que uma pontuação seja calculada para os grupos de métricas Temporal ou Ambiental, o grupo Métrica Base deve primeiro ser concluído. Em seguida, os valores de métrica Temporal e Ambiental modificam os resultados da Métrica Base para fornecer uma pontuação geral. A interação das pontuações para os grupos métricos é mostrada na figura.



A imagem mostra a interação de pontuações para os grupos métricos. No canto superior esquerdo do gráfico estão as Métricas de Grupo de Métricas Base, definidas pelo fornecedor: uma vez definida não muda. Uma seta conecta as Métricas a uma nuvem que representa a fórmula base. Uma seta aponta da nuvem para um círculo que representa a pontuação base. À esquerda, sob o Grupo de Métricas Base está o Grupo de Métricas Temporais, definido pelo fornecedor: uma vez definido, muda com o tempo. Uma seta conecta as Métricas de Grupo de Métricas Temporais a outra nuvem, representando a fórmula temporal. A fórmula temporal usa as Métricas Temporais e a Pontuação Base para criar a Pontuação Ajustada Temporariamente. À esquerda, sob o Grupo de Métricas Temporais, estão as Métricas de Grupo de Métricas Ambientais, opcionalmente definidas pelos usuários finais. Uma seta conecta as métricas de Grupo de Métricas Ambientais a uma nuvem que representa a Fórmula Ambiental. A Fórmula Ambiental usa as Métricas do Grupo de Métricas Ambientais e a pontuação Ajustada Temporariamente para criar a Pontuação Ajustada Ambiental. Fonte: [www.first.org](http://www.first.org)

Pontuação BasePontuação Ajustada TemporariamentePontuação Ambiental AjustadaFórmula BaseTemp. FórmulaEnv. FórmulaMétricasMétricasMétricas**Grupo de Métricas Base**   
Conjunto por fornecedor: uma vez definido, não muda.**Grupo de Métricas Temporais**   
Conjunto por fornecedor: uma vez definido, muda com o tempo.**Grupo de Métricas Ambientais Definido**   
opcionalmente pelos usuários finais.Fonte: www.first.org

23.2.5

## Relatórios CVSS

Os intervalos de escores e o significado qualitativo correspondente são mostrados na tabela.

| **Classificação** | **Pontuação CVSS** |
| --- | --- |
| Nenhum | 0 |
| Baixa | 0.1 – 3.9 |
| Médio | 4.0 – 6.9 |
| Alto | 7.0 – 8.9 |
| Críticos | 9.0 – 10.0 |

Frequentemente, as pontuações do grupo de métricas Base e Temporal serão fornecidas aos clientes pelo aplicativo ou fornecedor de segurança em cujo produto a vulnerabilidade foi descoberta. A organização afetada completa o grupo de métricas ambientais para adaptar a pontuação fornecida pelo fornecedor ao contexto local.

A pontuação resultante serve para orientar a organização afetada na alocação de recursos para resolver a vulnerabilidade. Quanto maior a classificação de gravidade, maior o impacto potencial de uma exploração e maior a urgência em abordar a vulnerabilidade. Embora não sejam tão precisos quanto os escores numéricos do CVSS, os rótulos qualitativos são muito úteis para se comunicar com os stakeholders que não conseguem se relacionar com os escores numéricos.

Em geral, qualquer vulnerabilidade que exceda 3.9 deve ser resolvida. Quanto maior o nível de classificação, maior a urgência para remediação.

23.2.6

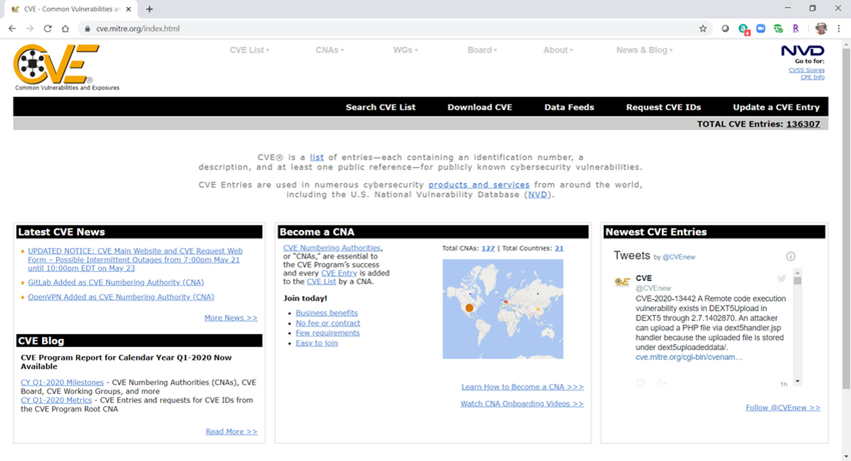
## Outras fontes de informações sobre vulnerabilidades

Existem outras fontes importantes de informações sobre vulnerabilidades. Estes trabalham em conjunto com o CVSS para fornecer uma avaliação abrangente da gravidade da vulnerabilidade. Existem dois sistemas que operam nos Estados Unidos:

**Vulnerabilidades e exposições comuns (CVE)**

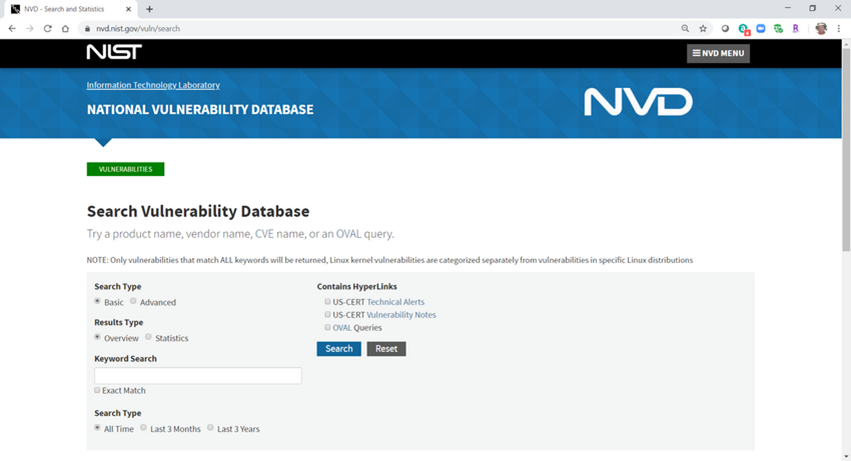
Este é um dicionário de nomes comuns, na forma de identificadores CVE, para vulnerabilidades conhecidas de segurança cibernética. O identificador CVE fornece uma maneira padrão de pesquisar uma referência a vulnerabilidades. Quando uma vulnerabilidade for identificada, identificadores CVE podem ser usados para acessar correções. Além disso, os serviços de inteligência contra ameaças usam identificadores CVE e aparecem em vários logs do sistema de segurança. O site Detalhes do CVE fornece uma ligação entre as pontuações do CVSS e as informações do CVE. Ele permite a navegação de registros de vulnerabilidade CVE por classificação de gravidade CVSS.

Pesquise Mitre na internet para obter mais informações sobre CVE como mostrado na figura.



**National Vulnerability Database (NVD)**

Isso utiliza identificadores CVE e fornece informações adicionais sobre vulnerabilidades, como pontuações de ameaças CVSS, detalhes técnicos, entidades afetadas e recursos para investigação adicional. O banco de dados foi criado e é mantido pela agência do National Institute of Standards and Technology (NIST) do governo dos EUA.



# Gerenciamento seguro de dispositivos

23.3.1

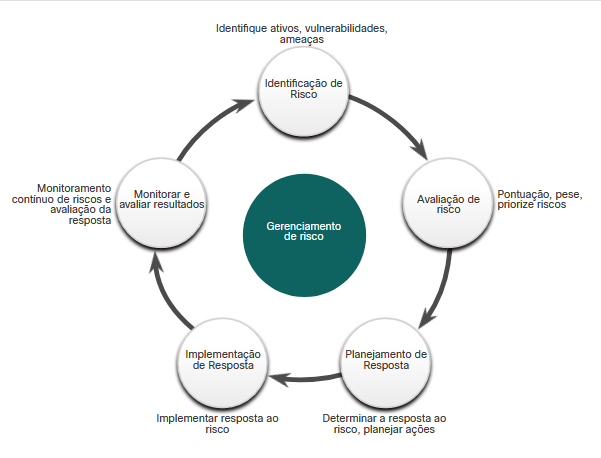
## Gerenciamento de risco

O gerenciamento de riscos envolve a seleção e especificação de controles de segurança para uma organização. Faz parte de um programa contínuo de segurança da informação em toda a organização que envolve a gestão do risco para a organização ou para indivíduos associados à operação de um sistema.

A gestão de riscos é um processo contínuo, multi-passo, cíclico, como mostrado na figura.

Imagem é um diagrama do Processo de Gestão de Riscos. Existem cinco pequenos círculos, organizados em um círculo representando o processo de gestão de riscos. Cada círculo é conectado ao próximo por setas apontando no sentido horário. Dentro do círculo superior está a Identificação de Riscos: identifique ativos, vulnerabilidades, ameaças. No segundo círculo está a Avaliação de Risco: pontuação, pese, priorize riscos. No terceiro círculo é o Planejamento de Resposta de Risco: determinar a resposta de risco, planejar ações. No quarto círculo é a Implementação de Resposta: implementar a resposta. No quinto círculo está Monitorar e Avaliar Resultados: monitoramento contínuo do risco e avaliação da resposta. A seta aponta de volta para a primeira caixa.

### Um processo de gestão de riscos



Identificação de RiscoImplementação de RespostaPlanejamento de RespostaMonitorar e avaliar resultadosAvaliação de riscoGerenciamento de riscoIdentifique ativos, vulnerabilidades, ameaçasMonitoramento contínuo de riscos e avaliação da respostaPontuação, pese, priorize riscosDeterminar a resposta ao risco, planejar açõesImplementar resposta ao risco

O risco é determinado como a relação entre ameaça, vulnerabilidade e a natureza da organização. Trata-se, em primeiro lugar, de responder às seguintes questões como parte de uma avaliação de risco:

* Quem são os atores que querem nos atacar?
* Quais vulnerabilidades os atores ameaçadores podem explorar?
* Como seríamos afetados por ataques?
* Qual é a probabilidade de que diferentes ataques ocorram?

A publicação especial 800-30 do NIST descreve a avaliação de risco como:

... o processo de identificação, estimativa e priorização dos riscos de segurança das informações. A avaliação do risco requer uma análise cuidadosa das informações sobre ameaças e vulnerabilidades para determinar a extensão em que circunstâncias ou eventos podem afetar negativamente uma organização e a probabilidade de tais circunstâncias ou eventos ocorrerem.

A publicação completa está disponível para download no NIST.

Uma atividade obrigatória na avaliação de riscos é a identificação de ameaças e vulnerabilidades e a correspondência de ameaças com vulnerabilidades no que geralmente é chamado de emparelhamento de ameaças (T-V). Os pares T-V podem então ser usados como uma linha de base para indicar o risco antes de os controles de segurança serem implementados. Esta linha de base pode, então, ser comparada com avaliações de risco contínuas como meio de avaliar a eficácia da gestão do risco. Esta parte da avaliação de risco é referida como a determinação do perfil de risco inerente de uma organização.

Após a identificação dos riscos, eles podem ser pontuados ou ponderados como forma de priorizar estratégias de redução de risco. Por exemplo, as vulnerabilidades que se verificou terem correspondido a várias ameaças podem receber classificações mais altas. Além disso, os pares T-V que mapeiam para o maior impacto institucional também receberão ponderações mais elevadas.

A tabela lista as quatro formas potenciais de responder aos riscos identificados, com base em suas ponderações ou pontuações.

| **Risco** | **Descrição** |
| --- | --- |
| **Prevenção de riscos** | * Pare de executar as atividades que criam risco. * É possível que, como resultado de uma avaliação de risco, se determine que o risco envolvido em uma atividade supera o benefício da atividade para a organização. * Se isso for considerado verdade, então pode-se determinar que a atividade deve ser descontinuada. |
| **Redução de risco** | * Diminua o risco tomando medidas para reduzir a vulnerabilidade. * Isso envolve a implementação de abordagens de gestão discutidas anteriormente neste capítulo. * Por exemplo, se uma organização usa sistemas operacionais de servidor que são freqüentemente direcionados por atores de ameaças, o risco pode ser reduzido por meio da garantia de que os servidores sejam corrigidos assim que as vulnerabilidades forem identificadas. |
| **Partilha de riscos** | * Mude parte do risco para outras partes. * Por exemplo, uma técnica de partilha de riscos pode ser terceirizar alguns aspectos das operações de segurança a terceiros. * A contratação de um CSIRT de segurança como serviço (SecaaS) para realizar o monitoramento de segurança é um exemplo. * Outro exemplo é comprar um seguro que ajudará a atenuar algumas das perdas financeiras devido a um incidente de segurança. |
| **Retenção de risco** | * Aceite o risco e suas conseqüências. * Esta estratégia é aceitável para riscos com baixo impacto potencial e custo relativamente elevado de mitigação ou redução. * Outros riscos que podem ser retidos são aqueles que são tão dramáticos que não podem ser realisticamente evitados, reduzidos ou compartilhados. |

23.3.2

## Verifique sua compreensão - identifique a resposta ao risco

Parte superior do formulário

1. Qual resposta ao risco aceita o risco e suas consequências?

Que resposta de risco terceirizará parte do risco para outras partes, como Segurança como Serviço?

Que resposta ao risco envolve a interrupção da realização das atividades de risco?

Qual resposta ao risco toma medidas para reduzir a vulnerabilidade?

23.3.3

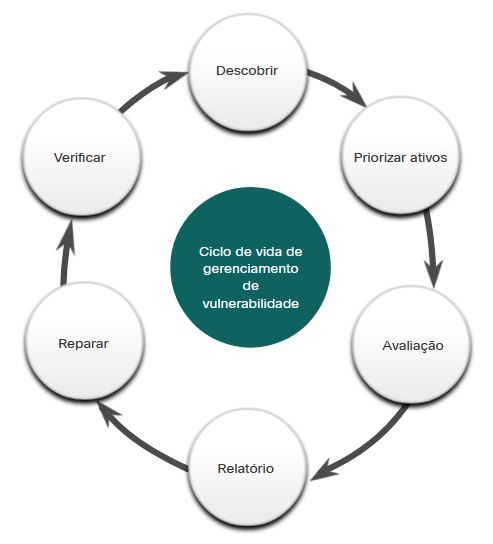
## Gerenciamento de vulnerabilidades

De acordo com o NIST, o gerenciamento de vulnerabilidades é uma prática de segurança projetada para impedir proativamente a exploração de vulnerabilidades de TI existentes em uma organização. O resultado esperado é reduzir o tempo e o dinheiro gasto para lidar com vulnerabilidades e a exploração dessas vulnerabilidades. O gerenciamento proativo de vulnerabilidades de sistemas reduzirá ou eliminará o potencial de exploração e envolverá consideravelmente menos tempo e esforço do que responder após uma exploração ter ocorrido.

O gerenciamento de vulnerabilidades requer um meio robusto de identificar vulnerabilidades com base em boletins de segurança do fornecedor e em outros sistemas de informação, como o CVE. O pessoal de segurança deve ser competente para avaliar o impacto, se houver, das informações de vulnerabilidade recebidas. As soluções devem ser identificadas com meios eficazes de implementar e avaliar as consequências imprevistas das soluções implementadas. Finalmente, a solução deve ser testada para verificar se a vulnerabilidade foi eliminada.

Imagem é um diagrama do Ciclo de Vida do Gerenciamento de Vulnerabilidades. Há seis pequenos círculos, organizados em um círculo maior, representando fases no Ciclo de Vida do Gerenciamento de Vulnerabilidades. Cada círculo é conectado ao próximo por setas apontando no sentido horário. As fases mostradas nos círculos são Descobrir, Priorizar ativos, Avaliar, Relatar, Remediar e Verificar. A última seta aponta de volta para a fase Descobrir.

### Ciclo de vida de gerenciamento de vulnerabilidade



**Descobrir** - Inventário de todos os ativos na rede e identifique os detalhes do host, incluindo sistemas operacionais e serviços abertos, para identificar vulnerabilidades. Desenvolva uma linha de base da rede. Identifique vulnerabilidades de segurança em um agendamento automatizado regular.

**Priorizar ativos** - Categorize os ativos em grupos ou unidades de negócios e atribua um valor comercial a grupos de ativos com base na sua importância às operações de negócios.

**Avaliação** - Determine um perfil de risco básico para eliminar riscos com base na importância, vulnerabilidade, ameaças e classificação de ativos.

**Relatório** - Meça o nível de risco comercial associado aos seus ativos de acordo com suas políticas de segurança. Documente um plano de segurança, monitore atividades suspeitas e descreva vulnerabilidades conhecidas.

**Reparar** - Priorize de acordo com o risco comercial e resolva vulnerabilidades por ordem de risco.

**Verificar** - Priorize de acordo com o risco comercial e resolva vulnerabilidades por ordem de risco.

23.3.4

## Gerenciamento de ativos

O gerenciamento de ativos envolve a implementação de sistemas que controlam a localização e a configuração de dispositivos e software em rede em uma empresa. Como parte de qualquer plano de gerenciamento de segurança, as organizações devem saber quais equipamentos acessam a rede, onde esse equipamento está dentro da empresa e logicamente na rede, e que software e dados esses sistemas armazenam ou podem acessar. O gerenciamento de ativos não apenas rastreia ativos corporativos e outros dispositivos autorizados, mas também pode ser usado para identificar dispositivos que não estão autorizados na rede.

O NIST especifica na publicação NISTIR 8011 Volume 2, os registros detalhados que devem ser mantidos para cada dispositivo relevante. O NIST descreve técnicas e ferramentas potenciais para operacionalizar um processo de gerenciamento de ativos:

* Detecção automatizada e inventário do estado real dos dispositivos
* Articulação do estado desejado para esses dispositivos usando políticas, planos e procedimentos no plano de segurança das informações da organização
* Identificação de ativos autorizados não conformes
* Remediação ou aceitação do estado do dispositivo, possível iteração da definição de estado desejado
* Repita o processo em intervalos regulares ou em curso

A figura fornece uma visão geral desse processo.

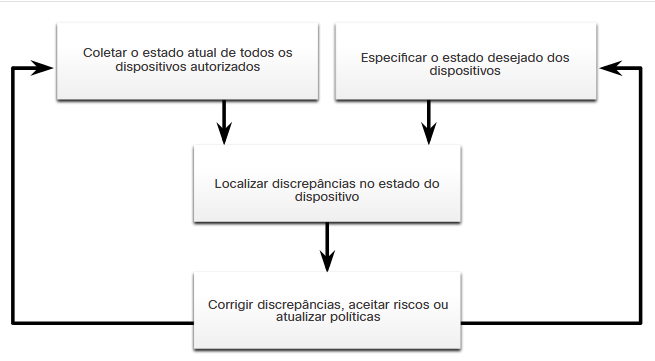


Figura é Um conceito operacional para gerenciamento de ativos com duas caixas de texto na parte superior rotuladas coletar estado atual de todos os dispositivos autorizados e especificar o estado desejado dos dispositivos. Cada uma dessas caixas de texto apontam para outra caixa de texto rotulada encontrar discrepâncias no estado do dispositivo. Esta caixa de texto aponta para outra caixa de texto rotulada discrepâncias corretas, aceitar riscos ou atualizar políticas. Esta última caixa de texto tem setas apontando para cada uma das duas caixas de texto superiores.

Coletar o estado atual de todos os dispositivos autorizadosEspecificar o estado desejado dos dispositivosLocalizar discrepâncias no estado do dispositivoCorrigir discrepâncias, aceitar riscos ou atualizar políticas

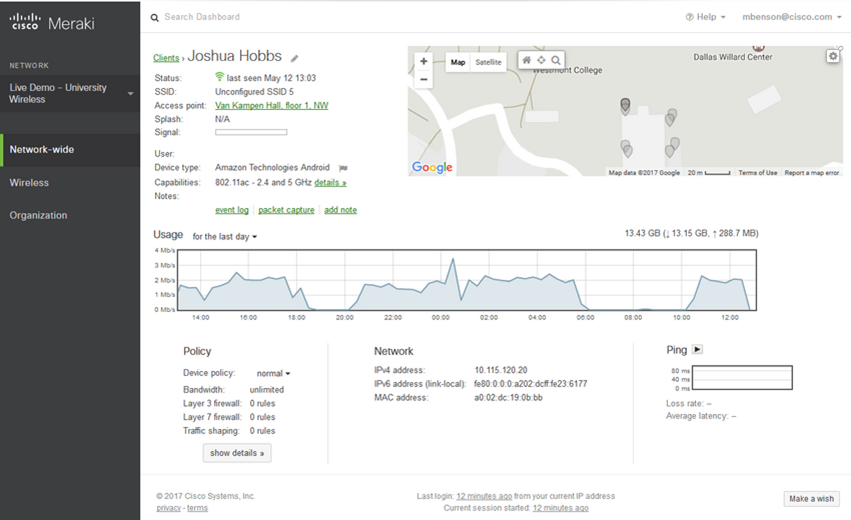
23.3.5

## Gerenciamento de dispositivos móveis (MDM)

O gerenciamento de dispositivos móveis (MDM), especialmente na era do BYOD, apresenta desafios especiais para a gestão de ativos. Os dispositivos móveis não podem ser controlados fisicamente nas instalações de uma organização. Elas podem ser perdidas, roubadas ou adulteradas, colocando em risco o acesso a dados e à rede. Parte de um plano MDM é agir quando os dispositivos deixam a custódia da parte responsável. As medidas que podem ser tomadas incluem desativar o dispositivo perdido, criptografar os dados no dispositivo e aprimorar o acesso ao dispositivo com medidas de autenticação mais robustas.

Devido à diversidade de dispositivos móveis, é possível que alguns dispositivos que serão usados na rede sejam inerentemente menos seguros do que outros. Os administradores de rede devem assumir que todos os dispositivos móveis não são confiáveis até que tenham sido adequadamente protegidos pela organização.

Os sistemas MDM, como o Cisco Meraki Systems Manager, mostrado na figura, permitem que o pessoal de segurança configure, monitore e atualize um conjunto muito diversificado de clientes móveis a partir da nuvem.



23.3.6

## ⁪Gerenciamento de configurações

O gerenciamento de configuração aborda o inventário e o controle das configurações de hardware e software dos sistemas. Configurações seguras de dispositivos reduzem o risco de segurança. Por exemplo, uma organização fornece muitos computadores e laptops para seus funcionários. Isso amplia a superfície de ataque para a organização, porque cada sistema pode ser vulnerável a explorações. Para gerenciar isso, a organização pode criar imagens de software de linha de base e configurações de hardware para cada tipo de máquina. Essas imagens podem incluir um pacote básico de software necessário, software de segurança de ponto de extremidade e políticas de segurança personalizadas que controlam o acesso do usuário a aspectos da configuração do sistema que poderiam ser tornados vulneráveis. As configurações de hardware podem especificar os tipos permitidos de interfaces de rede e os tipos permitidos de armazenamento externo.

O gerenciamento de configuração se estende à configuração de software e hardware de dispositivos de rede e servidores também. Conforme definido pelo NIST, gerenciamento de configuração:

Compreende uma coleção de atividades focadas no estabelecimento e manutenção da integridade de produtos e sistemas, através do controle dos processos de inicialização, alteração e monitoramento das configurações desses produtos e sistemas.

A publicação especial NIST 800-128 sobre gerenciamento de configuração para segurança de rede está disponível para download no NIST.

Para dispositivos de interrede, estão disponíveis ferramentas de software que farão backup de configurações, detectam alterações nos arquivos de configuração e habilitam a alteração em massa de configurações em vários dispositivos.

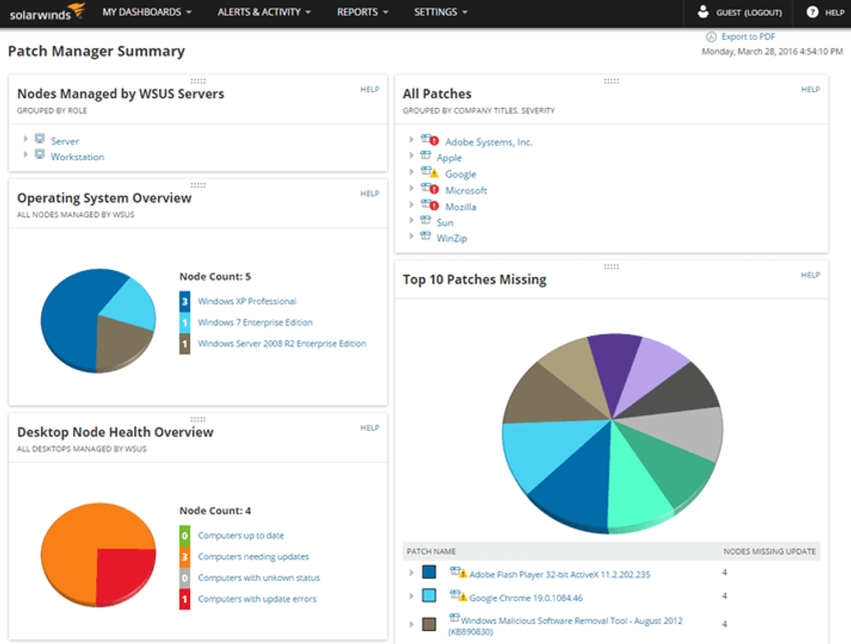
Com o advento dos data centers em nuvem e da virtualização, o gerenciamento de vários servidores apresenta desafios especiais. Ferramentas como Puppet, Chef, Ansible e SaltStack permitem o gerenciamento eficiente de servidores usados na computação baseada em nuvem.

23.3.7

## Gerenciamento Corporativo de Patchs

O gerenciamento de patches está relacionado ao gerenciamento de vulnerabilidades. Vulnerabilidades aparecem frequentemente em sistemas operacionais e firmware críticos de cliente, servidor e dispositivo de rede. Software de aplicativos, especialmente aplicativos de Internet e estruturas como Acrobat, Flash e Java, também são freqüentemente descobertos como tendo vulnerabilidades. O gerenciamento de patches envolve todos os aspectos da aplicação de patches de software, incluindo a identificação de patches necessários, aquisição, distribuição, instalação e verificação de que o patch está instalado em todos os sistemas necessários. A instalação de patches é frequentemente a maneira mais eficaz de mitigar vulnerabilidades de software. Às vezes, eles são a única maneira de fazê-lo.

O gerenciamento de patches é exigido por algumas regulamentações de conformidade, como Sarbanes Oxley (SOX) e a Lei de Portabilidade e Responsabilidade de Seguros de Saúde (HIPAA). A falha na implementação de patches de forma sistemática e oportuna pode resultar em falhas de auditoria e penalidades por não conformidade. O gerenciamento de patches depende dos dados de gerenciamento de ativos para identificar sistemas que executam software que exigem patches. O software de gerenciamento de patches está disponível em empresas como SolarWinds e LANDesk. O Microsoft System Center Configuration Manager (SCCM) é uma ferramenta de nível empresarial para distribuição automatizada de patches para um grande número de estações de trabalho e servidores Microsoft Windows.

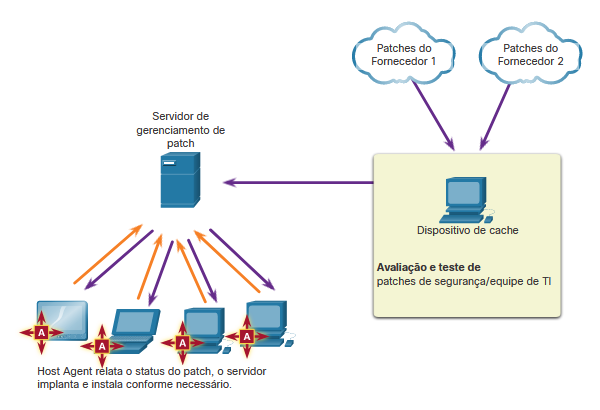


23.3.8

## técnicas de gerenciamento de patches

Baseado em agente

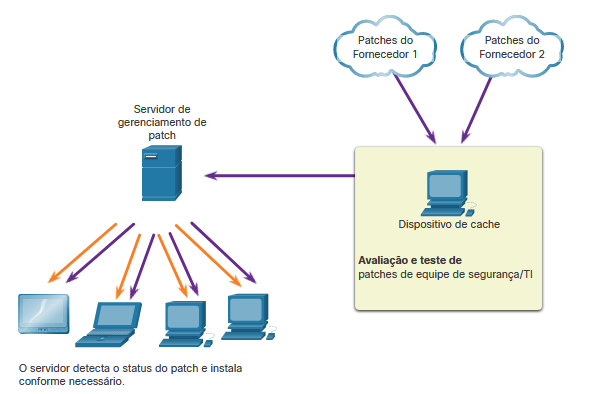
Isso requer que um agente de software esteja sendo executado em cada host a ser corrigido. O agente informa se o software vulnerável está instalado no host. O agente se comunica com o servidor de gerenciamento de patches, determina se existem patches que exigem instalação e instala os patches. O agente é executado com privilégios suficientes para permitir que ele instale os patches. As abordagens baseadas em agentes são os meios preferidos para a aplicação de patches em dispositivos móveis.



A figura mostra os patches baseados em agente com duas nuvens rotuladas como patches de fornecedor 1 e de fornecedor 2. Cada nuvem tem uma seta apontando para uma caixa que tem um PC rotulado dispositivo de cache e as palavras segurança/I T equipe avaliação patch e teste na parte inferior. Uma seta vai dessa caixa para o servidor de gerenciamento de patches. 2 PCs, um laptop e um dispositivo móvel têm um agente instalado e setas apontando para e do servidor de gerenciamento de patches e cada um desses dispositivos. As palavras Host Agent relata sobre o status do patch, o servidor implanta e instala conforme necessário estão abaixo dos dispositivos.

Varredura sem agente

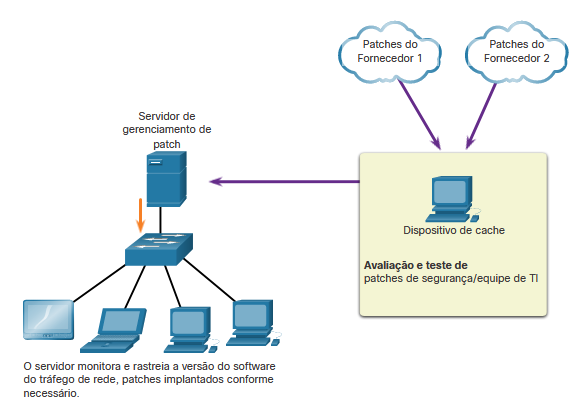
Os servidores de gerenciamento de patches verificam a rede em busca de dispositivos que exigem patches. O servidor determina quais patches são necessários e instala esses patches nos clientes. Somente os dispositivos que estão em segmentos de rede digitalizados podem ser corrigidos dessa maneira. Isso pode ser um problema para dispositivos móveis.



A figura mostra a varredura sem agente com a mesma topologia da baseada em agentes, mas as setas são diferentes. Neste, todas as setas estão longe do servidor de gerenciamento de patches apontando para os quatro dispositivos. As palavras são servidor detecta status do patch e instala conforme necessário.

Monitoramento da rede passivo

Os dispositivos que requerem aplicação de patches são identificados através do monitoramento do tráfego na rede. Essa abordagem só é eficaz para software que inclui informações de versão em seu tráfego de rede.



A Figura 3 é a mesma topologia, exceto que o servidor de gerenciamento de patches se conecta a um switch, bem como a todos os outros dispositivos ao mesmo switch. Há apenas uma seta que vai do servidor de gerenciamento de patches para o switch. As palavras na parte inferior são Monitores de servidor e rastreia a versão do software do tráfego de rede, patches implantados conforme necessário.

# Sistemas de Gestão de Segurança da Informação

23.4.1

## Sistemas de gerenciamento de segurança

Um Sistema de Gerenciamento de Segurança da Informação (ISMS) consiste em uma estrutura de gerenciamento por meio da qual uma organização identifica, analisa e aborda os riscos de segurança da informação. Os ISMSS não são baseados em servidores ou dispositivos de segurança. Em vez disso, um ISM consiste em um conjunto de práticas que são sistematicamente aplicadas por uma organização para garantir a melhoria contínua da segurança da informação. Os ISMSS fornecem modelos conceituais que orientam as organizações no planejamento, implementação, controle e avaliação de programas de segurança da informação.

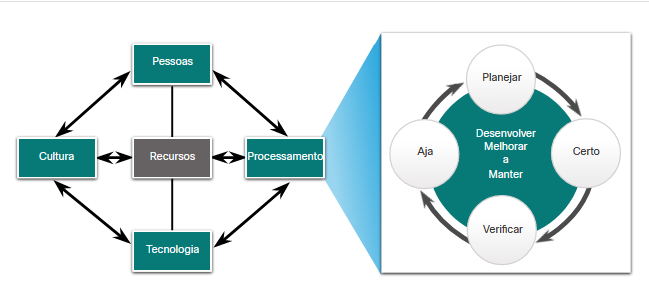
Os ISMSS são uma extensão natural do uso de modelos de negócios populares, como o Gerenciamento de Qualidade Total (TQM) e os Objetivos de Controle para a Informação e Tecnologias Relacionadas (COBIT), para o domínio da segurança cibernética.

Um ISMS é uma abordagem sistemática e multicamada para a segurança cibernética. A abordagem inclui pessoas, processos, tecnologias e as culturas em que interagem em um processo de gestão de riscos.

Um ISMS muitas vezes incorpora o framework “plan-do-check-act”, conhecido como o ciclo Deming, da TQM. É visto como uma elaboração sobre o componente processual do modelo de capacidade organizacional Povo-Process-Tecnologia-Cultura, como mostra a figura.

A imagem mostra um modelo geral de capacidade organizacional. O diagrama no lado esquerdo da imagem retrata o modelo Pessoas, Processo, Tecnologia, Cultura. Os quatro componentes do modelo são mostrados em um anel com capacidade no centro. Há setas apontando para ambos os lados entre todos os componentes. O componente Processo é expandido para outro gráfico no lado direito da imagem. Na exibição expandida, as quatro etapas na estrutura plano-do-check-act são mostradas em um círculo no sentido horário ao redor do texto: Desenvolver, Melhorar, Manter, ISMS.

### Um Modelo Geral para Capacidade Organizacional



23.4.2

## ISO-27001

ISO é a Organização Internacional de Padronização. Os padrões voluntários da ISO são internacionalmente aceitos e facilitam os negócios realizados entre as nações.

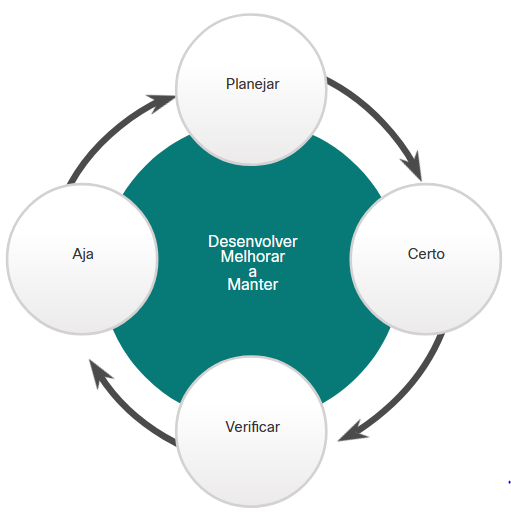
A ISO fez parceria com a Comissão Eletrotécnica Internacional (IEC) para desenvolver a série ISO/IEC 27000 de especificações para ISMSS, conforme mostrado na tabela.

| **Padrão** | **Descrição** |
| --- | --- |
| ISO/IEC 27000 | **Sistemas de gestão da segurança da informação — Visão geral e vocabulário** - Introdução à família de normas, visão geral do ISMS, vocabulário essencial. |
| ISO/IEC 27001 | **Sistemas de gestão da segurança da informação** **- Requisitos** - Fornece uma visão geral do ISMS e do essencial dos processos e procedimentos do ISMS. |
| ISO/IEC 27003 | **Orientação da implementação do sistema de gestão da segurança da informação** - Fatores críticos necessários para o sucesso do projeto e implementação do ISMS |
| ISO/IEC 27004 | **Gestão da segurança da informação - Monitoramento, medição, análise e avaliação** - Discussão de métricas e procedimentos de mensuração para avaliar a eficácia da implementação do ISM. |
| ISO/IEC 27005 | **Gestão de riscos de segurança da informação** - Apoia a implementação do ISMS com base numa abordagem de gestão centrada no risco. |

A certificação ISO 27001 é uma especificação global de todo o setor para um ISM. A figura ilustra a relação das ações estipuladas pelo padrão com o ciclo plano-do-check-act.

Na figura, as quatro etapas na estrutura plano-do-check-act são mostradas em um círculo no sentido horário em torno do texto: Desenvolver, Melhorar, Manter, ISMS.

### ISO 27001 Ciclo de Planejamento de Check-Act



Planejar

* Entender os objetivos de negócios relevantes
* Definir escopo das atividades
* Acesse e gerencie o suporte
* Avaliar e definir o risco
* Realizar gerenciamento de ativos e avaliação de vulnerabilidades

Certo

* Criar e implementar um plano de gestão de riscos
* Estabelecer e aplicar políticas e procedimentos de gestão de riscos
* Treinar pessoal, alocar recursos

Verificar

* Monitorar a implementação
* Compilar relatórios
* Suporte a auditoria externa de certificação

Aja

* Auditoria contínua de processos
* Melhorar continuamente os processos
* Tomar medidas corretivas
* Tomar medidas preventivas

A certificação ISO-27001 significa que as políticas e procedimentos de segurança de uma organização foram verificados de forma independente para fornecer uma abordagem sistemática e proativa para gerenciar eficazmente os riscos de segurança para informações confidenciais do cliente.

23.4.3

## NIST Cybersecurity Framework

O NIST é muito eficaz na área de segurança cibernética, como vimos neste módulo. Mais padrões do NIST serão discutidos mais tarde no curso.

O NIST também desenvolveu a estrutura de segurança cibernética, que é semelhante às normas ISO/IEC 27000. A estrutura do NIST é um conjunto de padrões projetados para integrar padrões, diretrizes e práticas existentes para ajudar a gerenciar e reduzir melhor o risco de segurança cibernética. O quadro foi emitido pela primeira vez em fevereiro de 2014 e continua a ser desenvolvido.

O núcleo da estrutura consiste em um conjunto de atividades sugeridas para alcançar resultados específicos de segurança cibernética e referências exemplos de orientação para alcançar esses resultados. As funções principais, que são definidas na tabela, são divididas em categorias e subcategorias principais.

| **Função principal** | **Descrição** |
| --- | --- |
| **IDENTIFY** | Desenvolva um entendimento organizacional para gerenciar o risco de segurança cibernética para sistemas, ativos, dados e recursos. |
| **PROTECT** | Desenvolver e implementar as salvaguardas adequadas para garantir a prestação de serviços de infraestrutura crítica. |
| **DETECT** | Desenvolver e implementar as atividades apropriadas para identificar a ocorrência de um evento de segurança cibernética. |
| **RESPOND** | Desenvolver e implementar as atividades apropriadas para agir em um evento de segurança cibernética detectado. |
| **RECOVER** | Desenvolver e implementar as atividades apropriadas para manter planos de resiliência e restaurar quaisquer capacidades ou serviços que tenham sido prejudicados devido a um evento de segurança cibernética. |

As principais categorias fornecem uma compreensão dos tipos de atividades e resultados relacionados a cada função, conforme mostrado na tabela seguinte.

| **Função principal** | **Categorias de Resultado** |
| --- | --- |
| **IDENTIFY** | * Gerenciamento de ativos * Ambiente de negócios * Governança * Avaliação de risco * Estratégia de Gestão de Risco |
| **PROTECT** | * Gerenciamento de identidade e controle de acesso * Processos e procedimentos de proteção de informações * Manutenção * Tecnologia de Proteção |
| **DETECT** | * Anomalias e Eventos * Monitoramento contínuo de segurança * Processos de detecção |
| **RESPOND** | * Planejamento de resposta * Comunicações * Análise * Atenuação * Melhorias |
| **RECOVER** | * Planejamento de Recuperação * Melhorias * Comunicações |

Organizações de muitos tipos estão usando o Framework de várias maneiras. Muitos acharam útil para aumentar a conscientização e se comunicar com as partes interessadas dentro de sua organização, incluindo a liderança executiva. O Framework também está melhorando as comunicações entre as organizações, permitindo que as expectativas de segurança cibernética sejam compartilhadas com parceiros de negócios, fornecedores e entre setores. Ao mapear o Framework para as abordagens atuais de gerenciamento de segurança cibernética, as organizações estão aprendendo e mostrando como elas correspondem aos padrões, diretrizes e práticas recomendadas do Framework. Algumas partes estão a utilizar o Quadro para conciliar a política interna com a legislação, a regulamentação e as melhores práticas da indústria. O Quadro também está sendo usado como uma ferramenta de planejamento estratégico para avaliar os riscos e as práticas atuais.

Pesquise na Internet para saber mais sobre o NIST Cybersecurity Framework.

# Resumo da avaliação de vulnerabilidade de endpoint

23.5.1

## O que aprendi neste módulo?

**Perfil de rede e servidor**

É importante executar o perfil de rede e dispositivo para fornecer informações estatísticas de linha de base que podem servir como um ponto de referência para o desempenho normal da rede e do dispositivo. Elementos importantes do perfil de rede incluem duração da sessão, taxa de transferência total, portas usadas e espaço de endereço de ativos críticos. A definição de perfil do servidor é usada para estabelecer o estado operacional aceito dos servidores. Um perfil de servidor é uma linha de base de segurança para um determinado servidor. Estabelece os parâmetros de rede, usuário e aplicativo que são aceitos para um servidor específico. O comportamento da rede é descrito por uma grande quantidade de dados diversos, como os recursos do fluxo de pacotes, os recursos dos próprios pacotes e a telemetria de várias fontes. A análise de Big Data pode ser usada para realizar a detecção de anomalias estatísticas, comportamentais e baseadas em regras.

A segurança de rede pode ser avaliada usando uma variedade de ferramentas e serviços. Análise de risco é a avaliação do risco representado por vulnerabilidades a uma organização específica. A avaliação de vulnerabilidades usa software para verificar servidores voltados para a Internet e redes internas em busca de vários tipos de vulnerabilidades. O teste de penetração usa ataques simulados autorizados para testar a força da segurança da rede.

**Sistema de pontuação de vulnerabilidade comum (CVSS)**

O Common Vulnerability Scoring System (CVSS) é uma estrutura aberta de padrão do setor neutro para classificar os riscos de uma determinada vulnerabilidade usando uma variedade de métricas para calcular uma pontuação composta. O CVSS produz pontuações padronizadas de vulnerabilidade que devem ser significativas em todas as organizações. É uma estrutura aberta com o significado de cada métrica abertamente disponível para todos os usuários. Ele permite priorizar o risco de uma forma que seja significativa para organizações individuais. O CVSS utiliza três grupos de métricas para avaliar a vulnerabilidade. Os grupos métricos são o grupo métrico base, o grupo de métricas temporais e o grupo de métricas ambientais. O grupo métrico base foi concebido como uma forma de avaliar vulnerabilidades de segurança encontradas em sistemas de software e hardware. As vulnerabilidades são classificadas de acordo com o vetor de ataque, a complexidade do ataque, os privilégios necessários, a interação do usuário e o escopo. Os grupos temporal e ambiental modificam o escore métrico base de acordo com o histórico da vulnerabilidade e o contexto da organização específica. Uma ferramenta de calculadora CVSS está disponível no site FIRST. A calculadora CVSS produz um número que descreve a gravidade do risco que é colocado pela vulnerabilidade. As pontuações variam de zero a dez. As faixas de escores apresentam valores qualitativos de risco nenhum, baixo, médio, alto ou crítico. Em geral, qualquer vulnerabilidade que exceda 3.9 deve ser resolvida. Quanto maior o nível de classificação, maior a urgência para remediação. Outras fontes importantes de informações de vulnerabilidade incluem Vulnerabilidades e Exposições Comuns (CVE) e o Banco de Dados Nacional de Vulnerabilidades (NVD), ambos disponíveis online.

**Gerenciamento de dispositivos seguros**

O gerenciamento de riscos envolve a seleção e especificação de controles de segurança para uma organização. Há quatro maneiras potenciais de responder aos riscos, evitar riscos significa interromper a atividade vulnerável, o sistema ou o serviço porque o risco é muito alto. Redução do risco significa tomar medidas para mitigar o risco, a fim de limitar o seu impacto. Partilha de riscos significa terceirização da responsabilidade pelo risco ou utilização de seguro para cobrir danos causados pelo risco. Retenção de riscos significa aceitar o risco e não tomar nenhuma ação.

O gerenciamento de vulnerabilidades é uma prática de segurança projetada para impedir proativamente a exploração de vulnerabilidades de TI existentes em uma organização. O ciclo de vida do gerenciamento de vulnerabilidades envolve seis etapas: descobrir, priorizar ativos, avaliar, relatar, corrigir e verificar. O gerenciamento de ativos envolve a implementação de sistemas que controlam a localização e a configuração de dispositivos e software em rede em uma empresa. Os sistemas de gerenciamento de dispositivos móveis (MDM) permitem que o pessoal de segurança configure, monitore e atualize um conjunto muito diversificado de clientes móveis a partir da nuvem. O gerenciamento de configuração aborda o inventário e o controle das configurações de hardware e software dos sistemas. O gerenciamento de patches está relacionado ao gerenciamento de vulnerabilidades e envolve todos os aspectos da aplicação de patches de software, incluindo a aquisição, distribuição, instalação e verificação de patches. O gerenciamento de patches é exigido por alguns regulamentos de conformidade. Existem diferentes técnicas de gerenciamento de patches, como varredura baseada em agente, sem agente e monitoramento passivo de rede.

**Sistemas de Gestão de Segurança da Informação**

As organizações podem usar um Sistema de Gerenciamento de Segurança da Informação (ISM) para identificar, analisar e lidar com os riscos de segurança das informações. Os padrões para gerenciamento de riscos de segurança cibernética estão disponíveis na ISO e no NIST. Um ISMS é uma abordagem sistemática e multicamada para a segurança cibernética que inclui pessoas, processos, tecnologias e as culturas em que interagem em um processo de gestão de riscos. A Organização Internacional de Normalização (ISO) fez parceria com a Comissão Eletrotécnica Internacional (IEC) para desenvolver a série ISO/IEC 27000 de especificações para ISMSS. O NIST também desenvolveu o Cybersecurity Framework, que é semelhante aos padrões ISO/IEC 27000. A estrutura do NIST é um conjunto de padrões projetados para integrar padrões, diretrizes e práticas existentes para ajudar a gerenciar e reduzir melhor o risco de segurança cibernética.