Princípios de Segurança da Informação

Prof. Me. Wallace Rodrigues de Santana

www.neutronica.com.br

Atribuição-NãoComercial-CompartilhaIgual 3.0 Brasil (CC BY-NC-SA 3.0)

Você tem a liberdade de:

Compartilhar — copiar, distribuir e transmitir a obra.

Remixar — criar obras derivadas.

Sob as seguintes condições:

Atribuição — Você deve creditar a obra da forma especificada pelo autor ou licenciante (mas não de maneira que sugira que estes concedem qualquer aval a você ou ao seu uso da obra).

Uso não comercial — Você não pode usar esta obra para fins comerciais.

Compartilhamento pela mesma licença — Se você alterar, transformar ou criar em cima desta obra, você poderá distribuir a obra resultante apenas sob a mesma licença, ou sob uma licença similar à presente.

Ficando claro que:

Renúncia — Qualquer das condições acima pode ser **renunciada** se você obtiver permissão do titular dos direitos autorais.

Domínio Público — Onde a obra ou qualquer de seus elementos estiver em **domínio público** sob o direito aplicável, esta condição não é, de maneira alguma, afetada pela licença.

Outros Direitos — Os seguintes direitos não são, de maneira alguma, afetados pela licença:

- Limitações e exceções aos direitos autorais ou quaisquer **usos livres** aplicáveis;
- Os **direitos morais** do autor;
- Direitos que outras pessoas podem ter sobre a obra ou sobre a utilização da obra, tais como **direitos de imagem** ou privacidade.

Aviso — Para qualquer reutilização ou distribuição, você deve deixar claro a terceiros os termos da licença a que se encontra submetida esta obra. A melhor maneira de fazer isso é com um link para esta página.

Módulo 9

Criptografia e certificados digitais

Introdução

Desde a antiguidade sempre houve a necessidade de se transmitir mensagens de forma que somente o destinatário pudesse acessá-la e compreendê-la.

Generais precisam dar ordens a seus comandados sem que essas caiam nas mãos do inimigo, e líderes políticos precisam trocar informações com seus aliados e estas devem estar a salvo de adversários.

Enfim, a arte de disfarçar, tornar secreta, codificar uma mensagem e transmiti-la de forma que somente o destinatário possa compreendê-la, evitando que qualquer outro possa roubar esta informação, tem sido vital em várias áreas.

Fonte: Fundação CECIERJ

Introdução

Existem duas formas básicas de proteger informações de forma que pessoas não autorizadas não tenham acesso ao seu conteúdo. São elas a esteganografia e a criptologia.

Esteganografia: deriva das palavras gregas *steganos*, que significa “coberto, oculto ou protegido”, e *gráphein* que significa “escrita”. Consiste na ocultação de mensagens dentro de outras mensagens. Um exemplo bastante comum é a utilização de imagens para a ocultação de textos.

Criptografia: deriva das palavras gregas *kryptós*, que significa “escondido ou secreto”, e *gráphein*, que significa “escrita”. Consiste de princípios e técnicas para transformar a informação de sua forma original para outra ilegível, de forma a proteger seu conteúdo do acesso de pessoas não autorizadas.

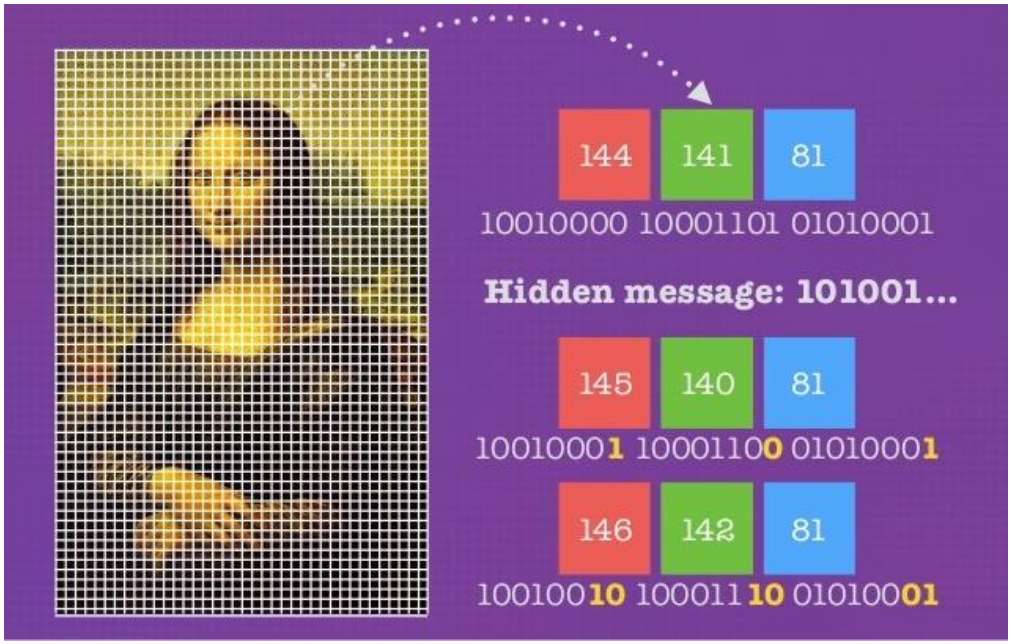
A diferença entre as duas é que a esteganografia oculta a existência da mensagem, enquanto a criptografia oculta o conteúdo da mesma. Pode-se utilizar as duas técnicas simultaneamente, cifrando uma mensagem e depois ocultando-a dentro de outra.

Fonte: Escola Superior de Redes RNP

Esteganografia

Muitas técnicas modernas possibilitam esconder informações dentro de imagens.

A forma mais utilizada emprega a técnica denominada LSB (Least Significant Bit, ou Bit Menos Significativo), que consiste em utilizar o bit menos significativo de uma determinada informação para armazenar um bit de uma nova informação.



Fonte: Wikipedia

Esteganografia

O Caso Abadia

Quando o traficante colombiano Juan Carlos Ramírez Abadía foi preso em São Paulo em agosto de 2007, os delegados da Polícia Federal ficaram intrigados com a quantidade de imagens da Hello Kitty que ele guardava nos computadores. Eram quase 200 imagens, quase todas enviadas por e-mail.

A perícia da Polícia Federal descobriu que haviam mensagens de voz e de texto escondidas nas imagens.

Fonte: Folha de São Paulo

Esteganografia – demonstração

Uma forma menos sutil de esconder mensagens em uma imagem é anexar um arquivo texto a uma imagem JPEG.

Pode-se usar o seguinte comando no console do Windows para combinar de forma binária os arquivos HelloKitty.jpg e Mensagem.txt no arquivo Desenho.jpg:

```
copy /b HelloKitty.jpg + Mensagem.txt Desenho.jpg
```

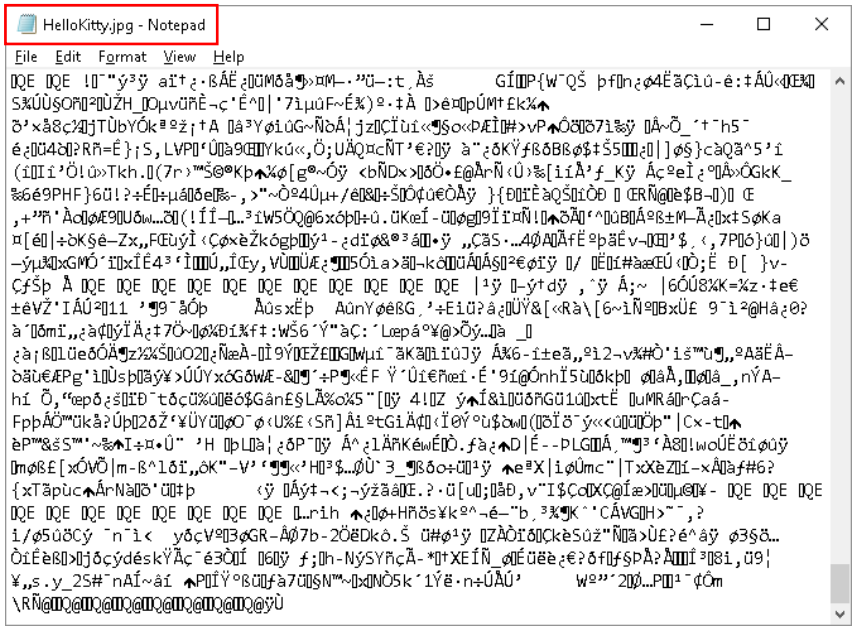
HelloKitty.jpg | Mensagem.txt | Desenho.jpg

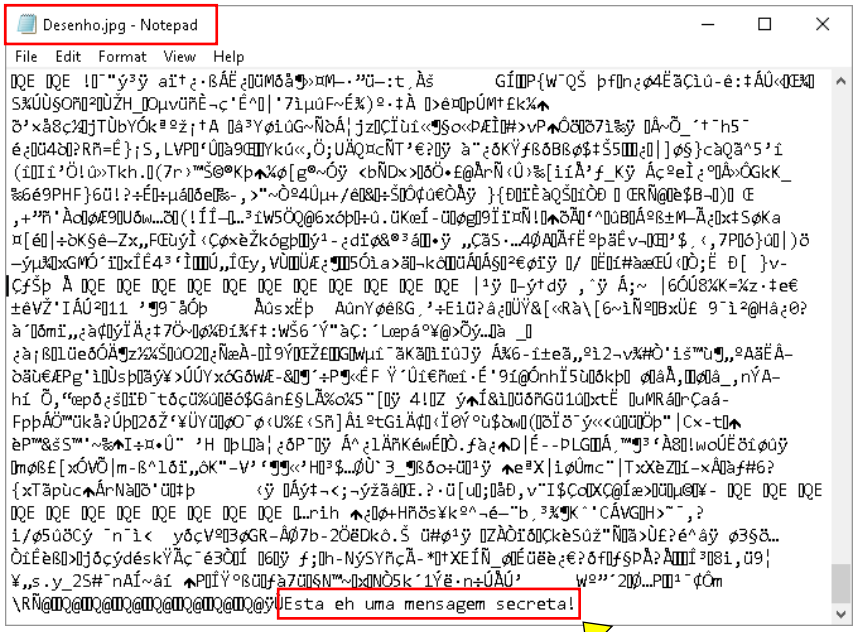
O arquivo Mensagem.txt possui o seguinte texto: Esta eh uma mensagem secreta!

Esteganografia – demonstração

Depois de realizada a cópia binária, basta abrir os dois arquivos no Bloco de Notas. A diferença entre eles poderá ser visualizada no final do arquivo.

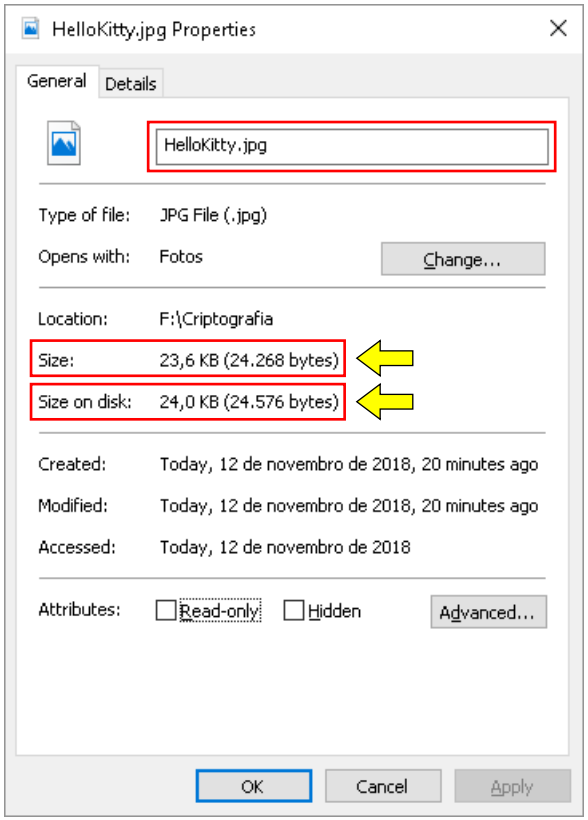
Se o usuário abrir estes dois arquivos em um visualizador de imagens, a diferença não poderá ser notada.

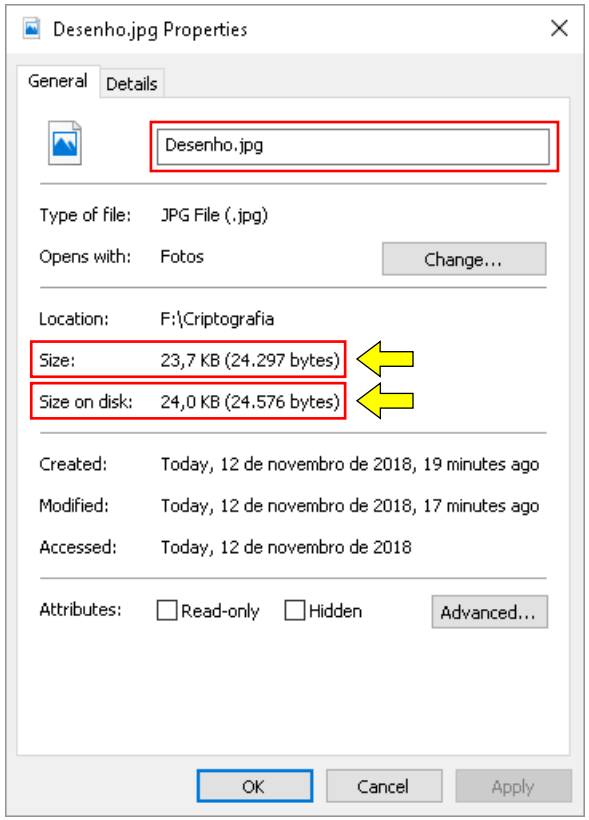




Esteganografia – demonstração

É possível verificar que o arquivo Desenho.jpg ficou ligeiramente maior que o arquivo original HelloKitty.jpg, uma vez que ele contém a mensagem escondida.





Criptografia

A criptografia, considerada como a ciência e a arte de escrever mensagens em forma cifrada ou em código, consiste em transformar a informação de sua forma original e legível para outra ilegível, protegendo assim de pessoas não autorizadas o acesso ao seu conteúdo.

É hoje um dos principais mecanismos de segurança que pode-se usar para proteger dos riscos associados ao uso da Internet.

Fonte: Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

Criptografia

Por meio do uso da criptografia pode-se:

- proteger os dados sigilosos armazenados no computador;
- criar uma área (partição) específica no computador, na qual todas as informações que forem lá gravadas serão automaticamente criptografadas;
- proteger os *backups* contra acesso indevido, principalmente aqueles enviados para áreas de armazenamento externo de mídias;
- proteger as comunicações realizadas pela Internet, como os *e-mails* enviados/recebidos e as transações bancárias e comerciais realizadas.

As técnicas básicas de criptografia por embaralhamento de mensagem são a transposição e a substituição.

Fonte: Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

Conceitos

REMETENTE: Pessoa ou serviço que envia a informação;

DESTINATÁRIO: Pessoa ou serviço que recebe a informação;

CANAL DE COMUNICAÇÃO: Meio utilizado para a troca de informações;

TEXTO CLARO: Informação legível (original) que será protegida, ou seja, que será cifrada;

TEXTO CIFRADO: Texto ilegível, gerado pela codificação de um texto claro;

CIFRAR: Ato de transformar um texto claro em um texto codificado;

DECIFRAR: Ato de transformar um texto codificado em um texto claro;

MÉTODO CRIPTOGRÁFICO: Conjunto de programas responsável por cifrar (codificar) e decifrar (decodificar) informações;

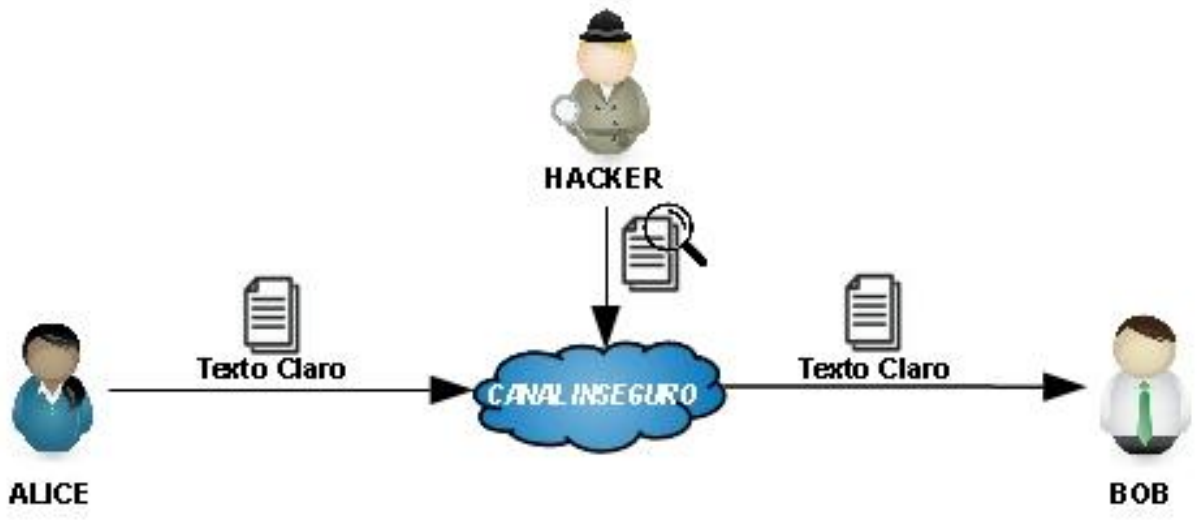
CHAVE: Similar a uma senha, é utilizada como elemento secreto pelos métodos criptográficos. Seu tamanho é geralmente medido em quantidade de bits;

ESPAÇO DE CHAVES: Quantidade de combinações possíveis de chave.

Fonte: Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

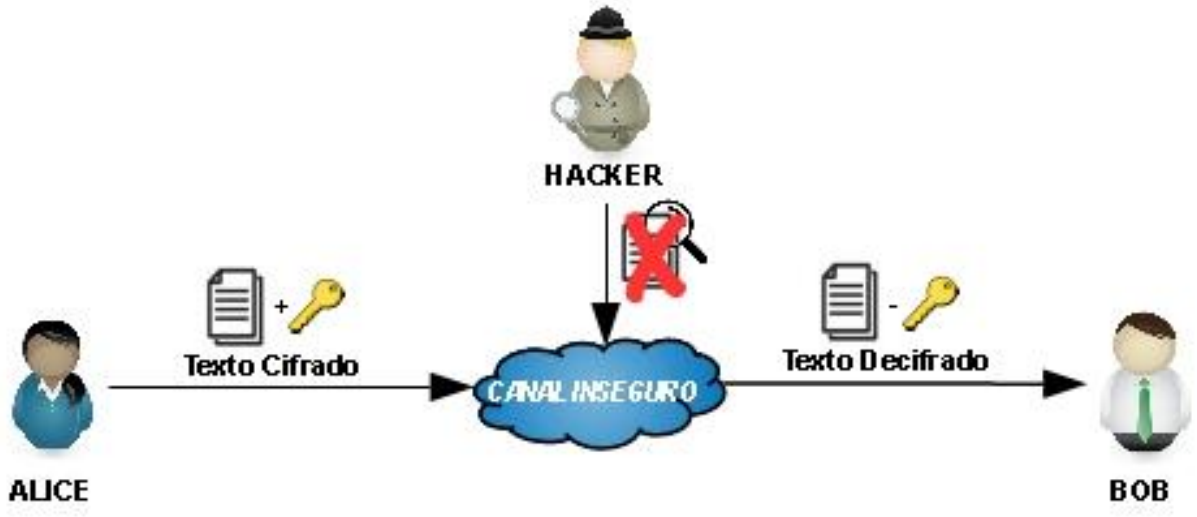
Troca de mensagens

Quando Alice deseja enviar uma mensagem para Bob por meio de um canal inseguro, um terceiro (Hacker) pode interceptar a mensagem e verificar o seu conteúdo.



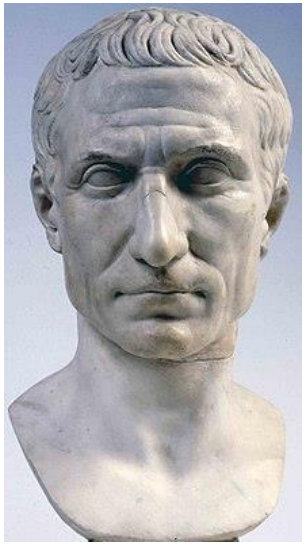
Troca de mensagens

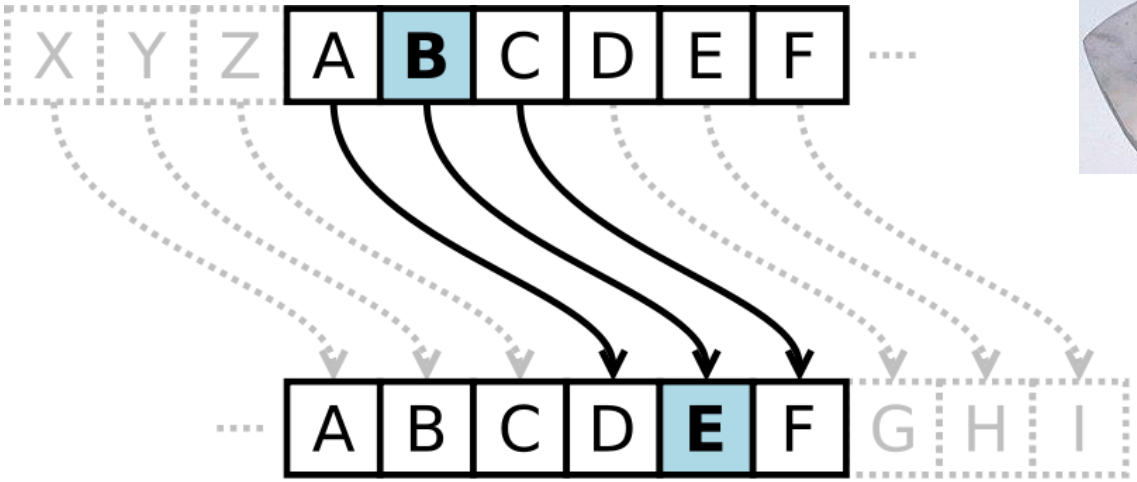
Uma forma de proteger a comunicação seria adotar um canal seguro onde somente Alice e Bob tivessem acesso, ou então codificar (cifrar) a mensagem de tal forma que um terceiro (Hacker) não conseguiria verificar o seu conteúdo, ainda que estivesse de posse da mensagem.



Cifra de César

O Imperador Romano Júlio César, que viveu de 100 AC à 44 AC, usava na sua correspondência militar uma chave de substituição muito simples, na qual cada letra da mensagem original era substituída pela letra que a seguia em três posições no alfabeto. A letra A era substituída pela D, a B pela E, e assim sucessivamente.



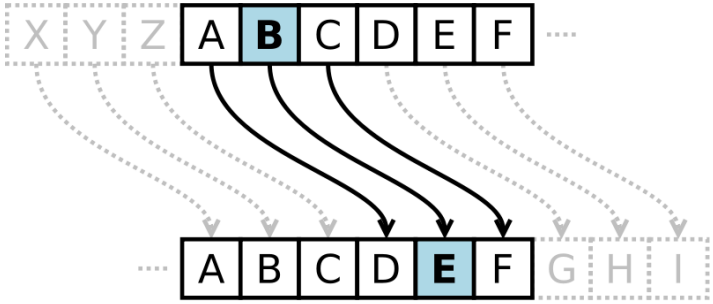


Fonte: Fundação CECIERJ

Cifra de César – algoritmo

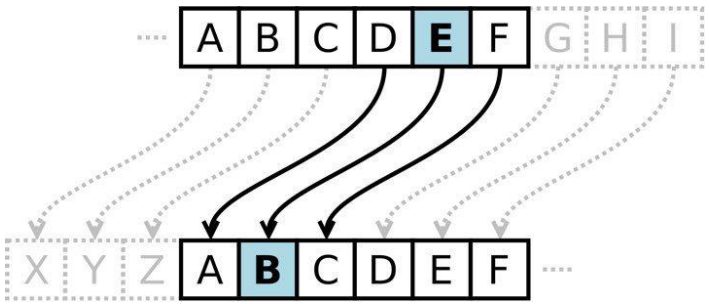
Para cifrar a mensagem, aplica-se a função de encriptação $E_k(x)$, onde x é a mensagem original e k a chave. Para decriptar a mensagem, usa-se a função $D_k(x)$.

ENCRIPTAR (CIFRAR)



$$E_k(x) = (x + k)\ mod\ 26$$

DECRIPTAR (DECIFRAR)



$$D_k(x) = (x - k)\ mod\ 26$$

⚠ Como a chave usada para encriptar e decriptar a mensagem é a mesma, a chamamos de **Chave Simétrica**.

⚠ Como o alfabeto usado possui 26 letras, significa que temos ***k-1*** (25) combinações possíveis, o que chamamos de **Espaço de Chaves**.

⚠ O operador ***mod 26*** (resto de divisão inteira) garante que a função seja limitada ao espaço de chaves do alfabeto.

Cifra de César – exemplo

**Leônidas I, Rei e General da cidade-estado de Esparta (491 AC à 480 AC).*

Cifra de César – exemplo

A RESISTENCIA SE DARA NO DESFILADEIRO DAS TERMOPILAS

operação[+] → chave[3]

D UHVLVWHQFLD VH GDUD QR GHVILODGHLUR GDV WHUPRSLODV

operação[-], chave[3]

A RESISTENCIA SE DARA NO DESFILADEIRO DAS TERMOPILAS

Cifra de César – força bruta

TEXTO CIFRADO

D UHVLVWHQFLD VH GDUD QR GHVILODGHLUR GDV WHUPRSLODV

FORÇA BRUTA

CHAVE	
-6	X OBPFPQBKZFX PB AXOX KL ABPCFIXABFOL AXP QBOJLMFIXP
-5	Y PCQGQRCLAGY QC BYPY LM BCQDGJYBCGPM BYQ RCPKMNGJYQ
-4	Z QDRHRSDMBHZ RD CZQZ MN CDREHKZCDHQN CZR SDQLNOHKZR
-3	A RESISTENCIA SE DARA NO DESFILADEIRO DAS TERMOPILAS
-2	B SFTJTUFODJB TF EBSB OP EFTGJMBEFJSP EBT UFSNPQJMBT
-1	C TGUKUVGPEKC UG FCTC PQ FGUHKNCFGKTQ FCU VGTOQRKNCU

Cifra de César – conclusão

O que garante a segurança do método criptográfico não é o seu algoritmo, mas sim o seu espaço de chaves!

Cifra de César – exercício

**Elfiates, filho de Euridemo de Malis e nascido em Traquis, na Tessália.*

Métodos criptográficos

De acordo com o tipo de chave usada, os métodos criptográficos podem ser subdivididos em duas grandes categorias:

- criptografia de chave simétrica;
- criptografia de chaves assimétricas.

Chave
Compartilhada

Chave Simétrica

A mesma chave compartilhada é usada para cifrar e decifrar a mensagem

Chave
Pública

Chave
Privada

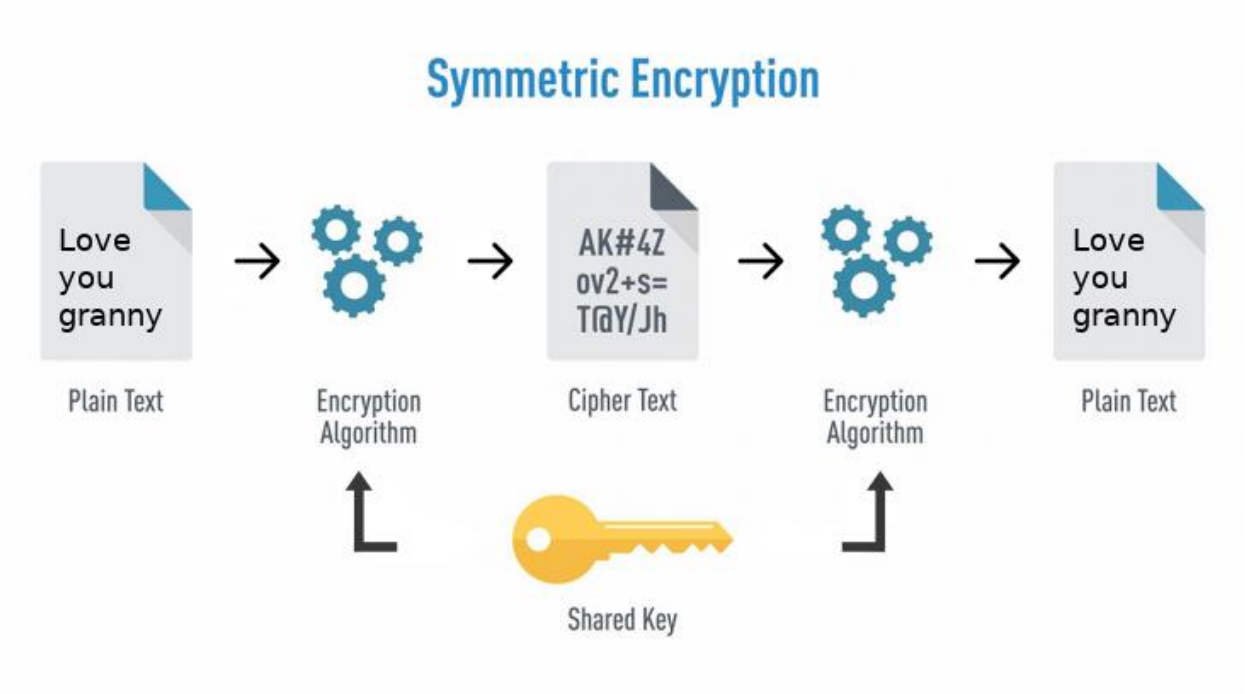
Chaves Assimétricas

São usadas duas chaves, uma para cifrar a mensagem (chave pública) e outra para decifrar (chave privada)

Fonte: Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

Criptografia de chave simétrica

Criptografia de chave simétrica ou criptografia de chave secreta ou única, utiliza uma mesma chave tanto para codificar como para decodificar informações, sendo usada principalmente para garantir a confidencialidade dos dados.



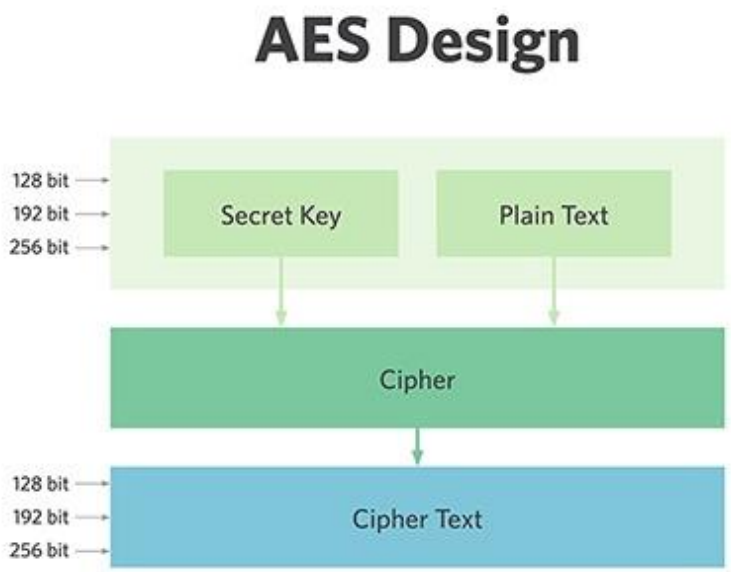
Fonte: Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

Criptografia de chave simétrica

Casos nos quais a informação é codificada e decodificada por uma mesma pessoa não há necessidade de compartilhamento da chave secreta. Entretanto, quando estas operações envolvem pessoas ou equipamentos diferentes, é necessário que a chave secreta seja previamente combinada por meio de um canal de comunicação seguro (para não comprometer a confidencialidade da chave).

Exemplos de algoritmos criptográficos que usam chave simétrica são:

- AES;
- Blowfish;
- RC4;
- 3DES;
- IDEA.



Fonte: Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

Criptografia de chave simétrica

A criptografia de chave simétrica, quando comparada com a de chaves assimétricas, é a mais indicada para garantir a confidencialidade de grandes volumes de dados, pois seu processamento é mais rápido.

Todavia, quando usada para o compartilhamento de informações, se torna complexa e pouco escalável, em virtude da:

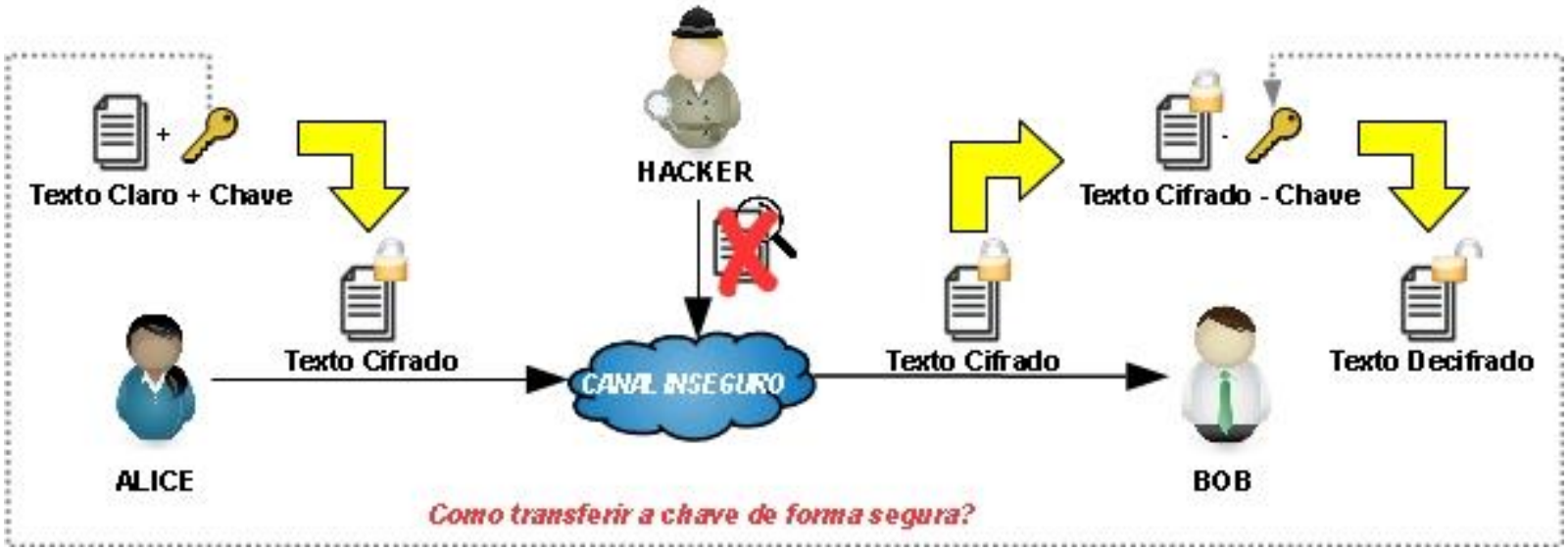
- necessidade de um canal de comunicação seguro para promover o compartilhamento da chave secreta entre as partes (o que na Internet pode ser bastante complicado);
- dificuldade de gerenciamento de grandes quantidades de chaves, uma vez que seriam necessárias várias chaves secretas distintas para cada pessoa com quem quisesse comunicar-se.

Fonte: Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

Criptografia de chave simétrica

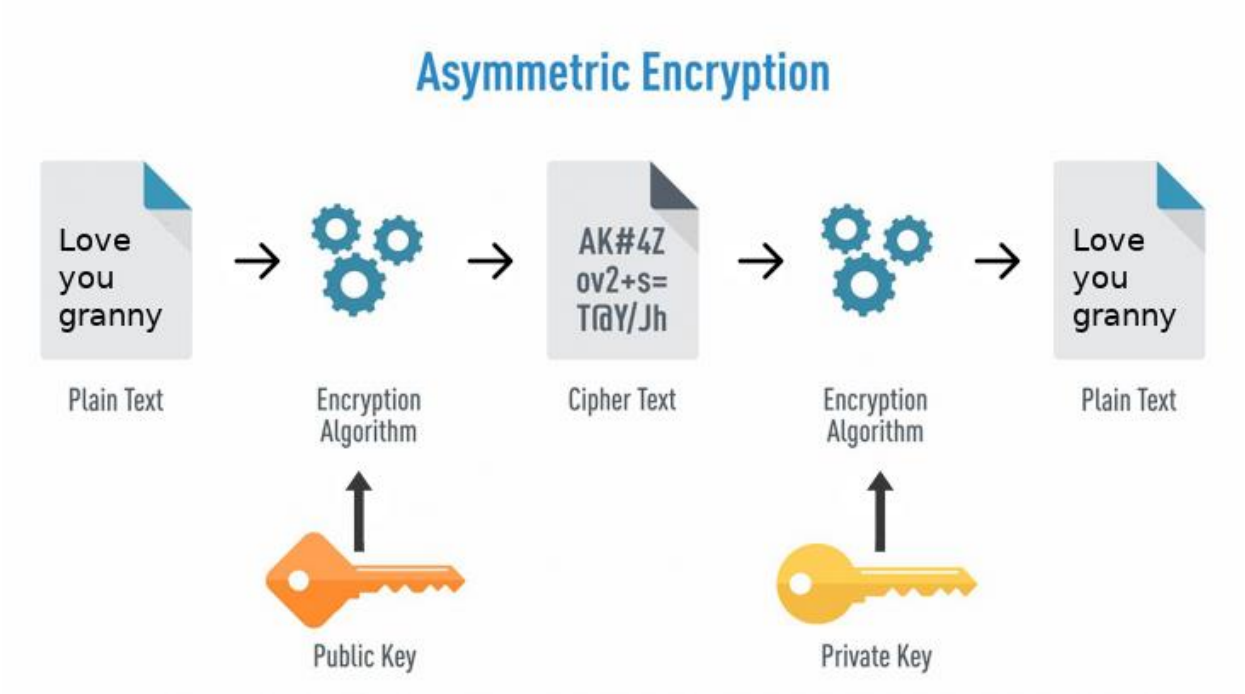
Para Alice enviar uma mensagem para Bob por meio de um canal inseguro, sem que um terceiro (Hacker) intercepte a mensagem e verifique o seu conteúdo, Alice deve cifrar a mensagem e compartilhar uma chave simétrica com Bob.

A questão que fica é: como transferir a chave simétrica de forma segura?



Criptografia de chaves assimétricas

Criptografia de chaves assimétricas, também conhecida como criptografia de chave pública, utiliza duas chaves distintas: uma pública, que pode ser livremente divulgada, e uma privada, que deve ser mantida em segredo por seu dono.



Fonte: Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

Criptografia de chaves assimétricas

Quando uma informação é codificada com uma das chaves, somente a outra chave do par pode decodificá-la. Qual chave usar para codificar depende da proteção que se deseja, se confidencialidade ou autenticação, integridade e não-repúdio.

A chave privada pode ser armazenada de diferentes maneiras, como um arquivo no computador, um *smartcard* ou um *token*, e a sua guarda é de responsabilidade de seu proprietário.

Já a chave pública pode ficar armazenada em um repositório de acesso público.

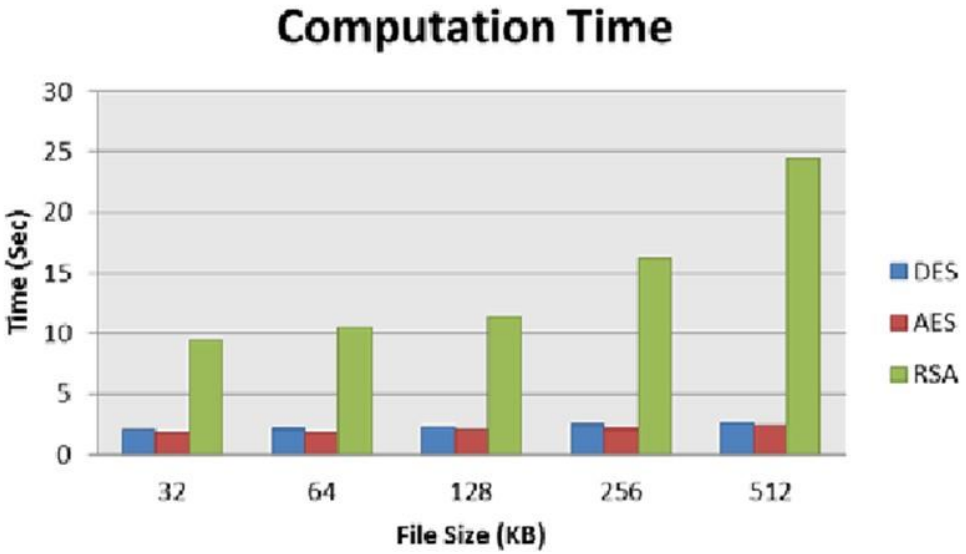
Exemplos de algoritmos criptográficos que usam chaves assimétricas são:

- RSA;
- DSA;
- ECC;
- Diffie-Hellman.

Fonte: Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

Criptografia de chaves assimétricas

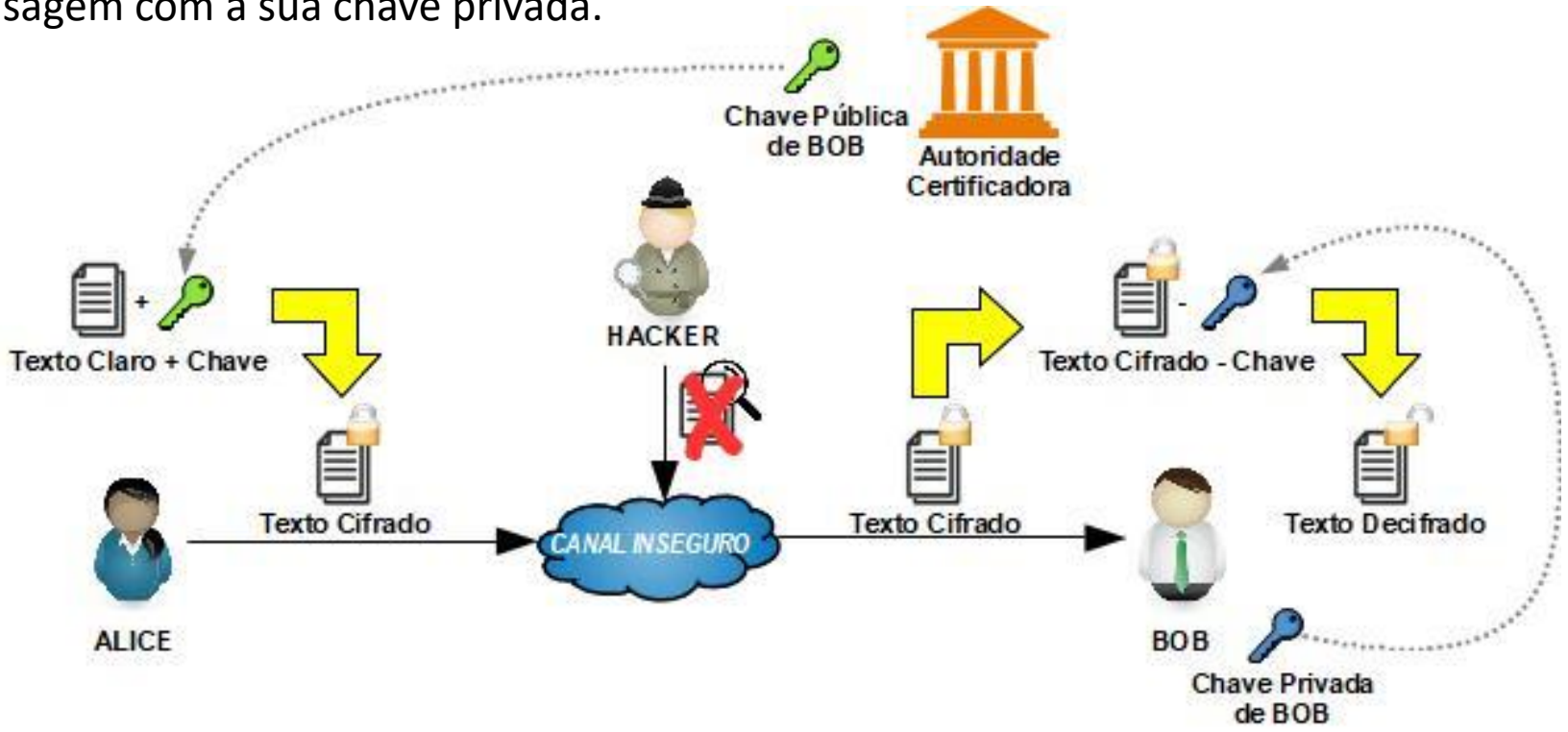
A criptografia de chaves assimétricas, apesar de possuir um processamento mais lento que a de chave simétrica, resolve os problemas de canal seguro e de gerenciamento de chaves, uma vez que facilita o seu gerenciamento (pois não requer que se mantenha uma chave secreta com cada um que desejar se comunicar) e dispensa a necessidade de um canal de comunicação seguro para o compartilhamento de chaves.



Fonte: Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

Criptografia de chaves assimétricas

Para Alice enviar uma mensagem para Bob por meio de um canal inseguro sem que um terceiro (Hacker) intercepte a mensagem e verifique o seu conteúdo, Alice deve cifrar a mensagem com a chave pública de Bob e este deve decifrar a mensagem com a sua chave privada.

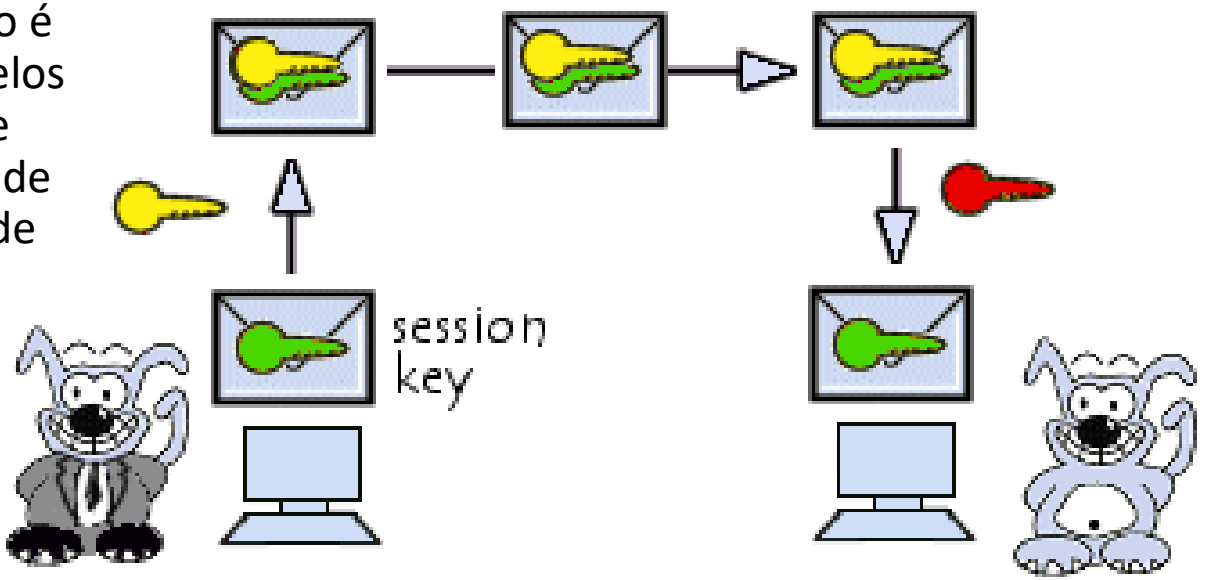


Criptografia – aplicações

Para aproveitar as vantagens dos métodos de chave simétrica e assimétricas, o ideal é o uso combinado de ambos, onde o primeiro é usado para codificar a informação e o segundo é utilizado para o compartilhamento da chave secreta (neste caso, também chamada de chave de sessão).

Este uso combinado é o que é utilizado pelos navegadores Web e programas leitores de e-mails. Exemplos de uso deste método combinado são:

- SSL;
- PGP;
- S/MIME.

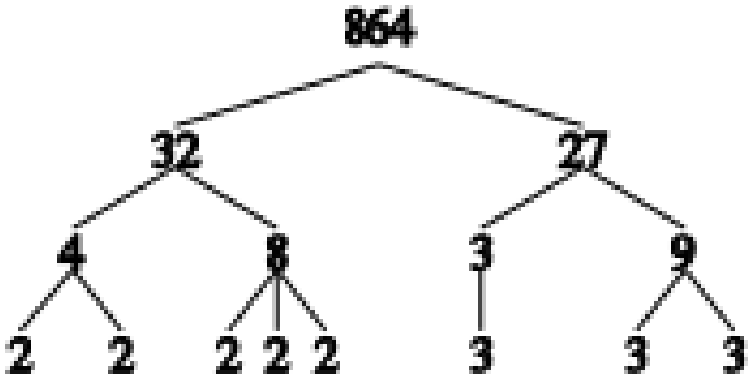


Fonte: Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

RSA

RSA (Rivest-Shamir-Adleman) é um sistema de criptografia de chave pública amplamente utilizado para transmissão segura de dados. Seu acrônimo vem dos sobrenomes dos criptógrafos Ron Rivest, Adi Shamir e Leonard Adleman, que descreveram o algoritmo em 1978.

Neste sistema de criptografia de chaves assimétricas, a assimetria é baseada na dificuldade prática da fatoração do produto de dois números primos grandes, conhecido como “problema de fatoração”.

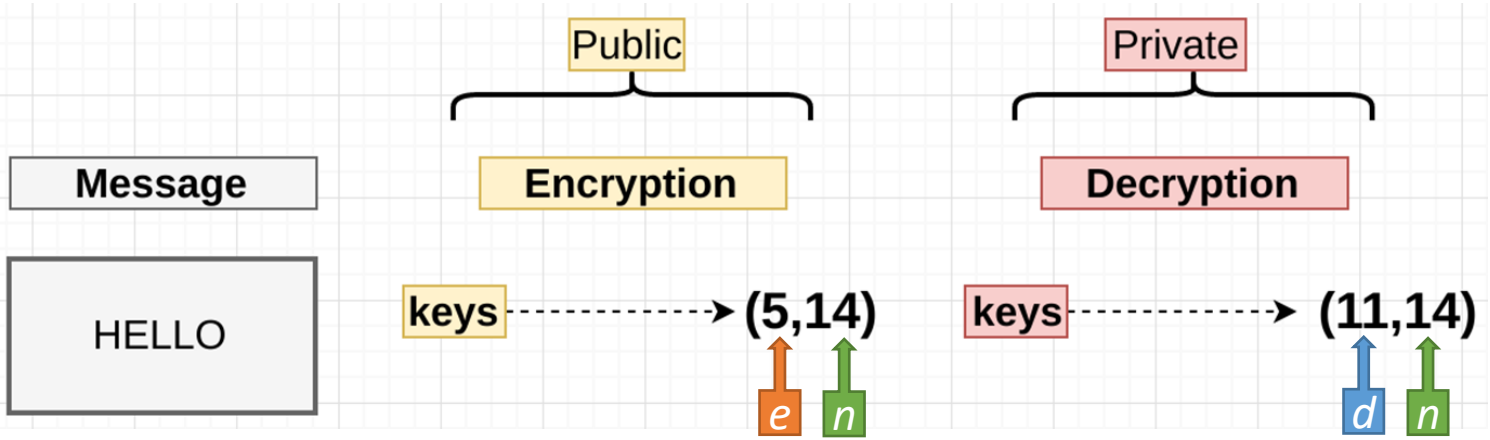


Fonte: www.wikipedia.org

RSA

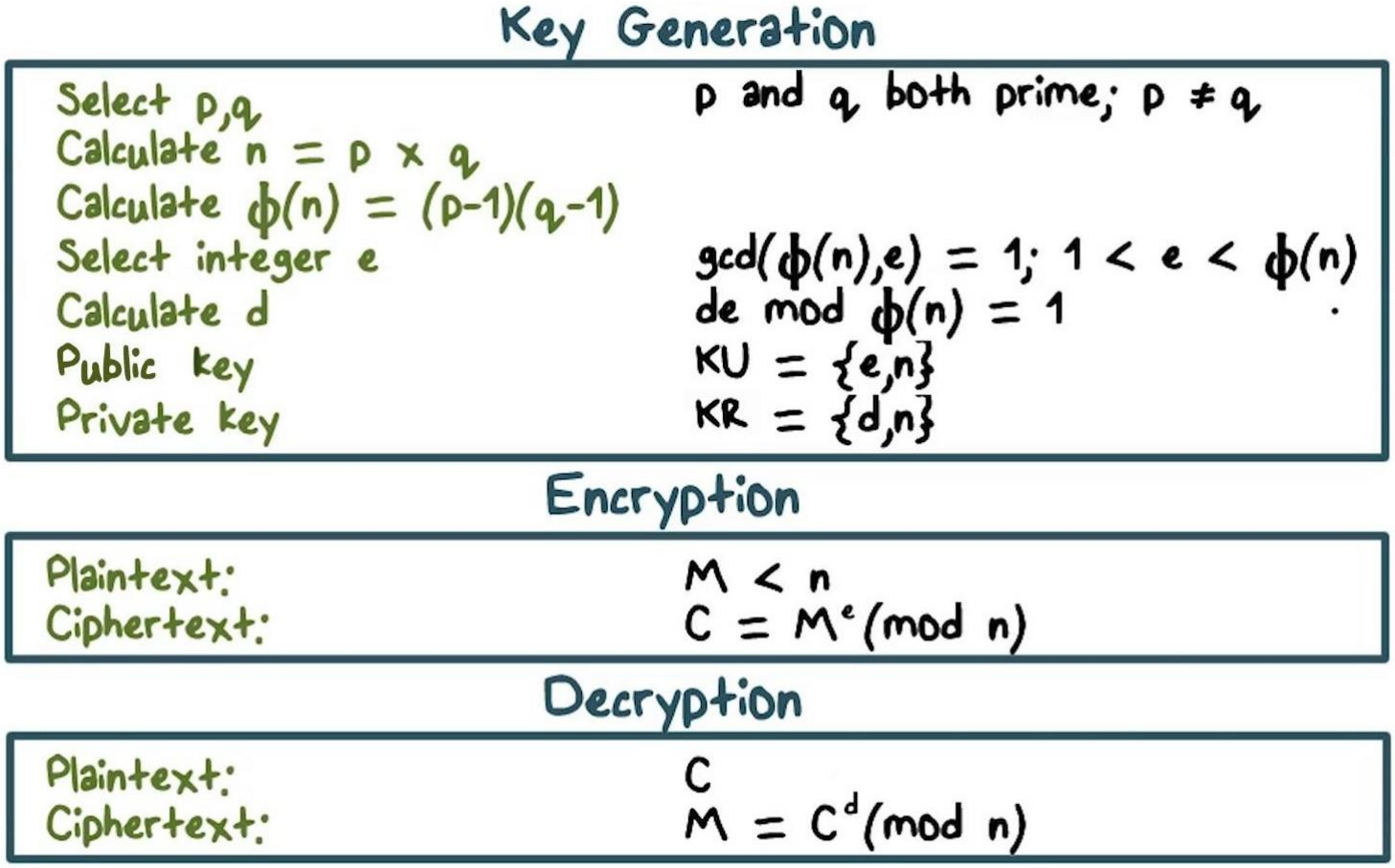
Um usuário do RSA cria e divulga uma chave pública composta pelo produto ***n*** de dois números primos grandes e por um valor auxiliar ***e***. Os números primos devem ser mantidos em segredo. Qualquer um pode usar a chave pública para cifrar a mensagem, mas para decifrá-la é necessária a chave privada composta por ***n*** e o número calculado ***d***, de conhecimento apenas do dono da chave.

Com os métodos atualmente conhecidos e se a chave pública for muito grande, só é possível decifrar a mensagem conhecendo-se os números primos usados originalmente. Quebrar a encriptação RSA é conhecido como problema RSA.



Fonte: www.wikipedia.org

RSA – algoritmo

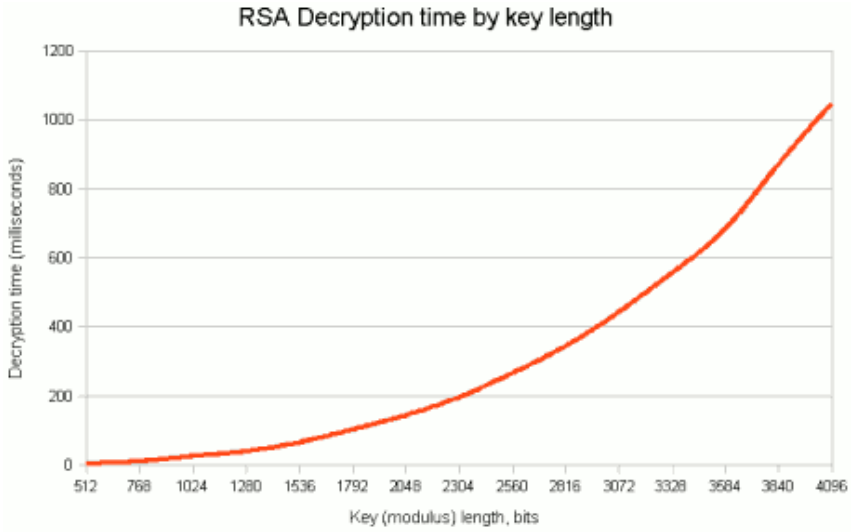


Fonte: www.digicert.com

RSA

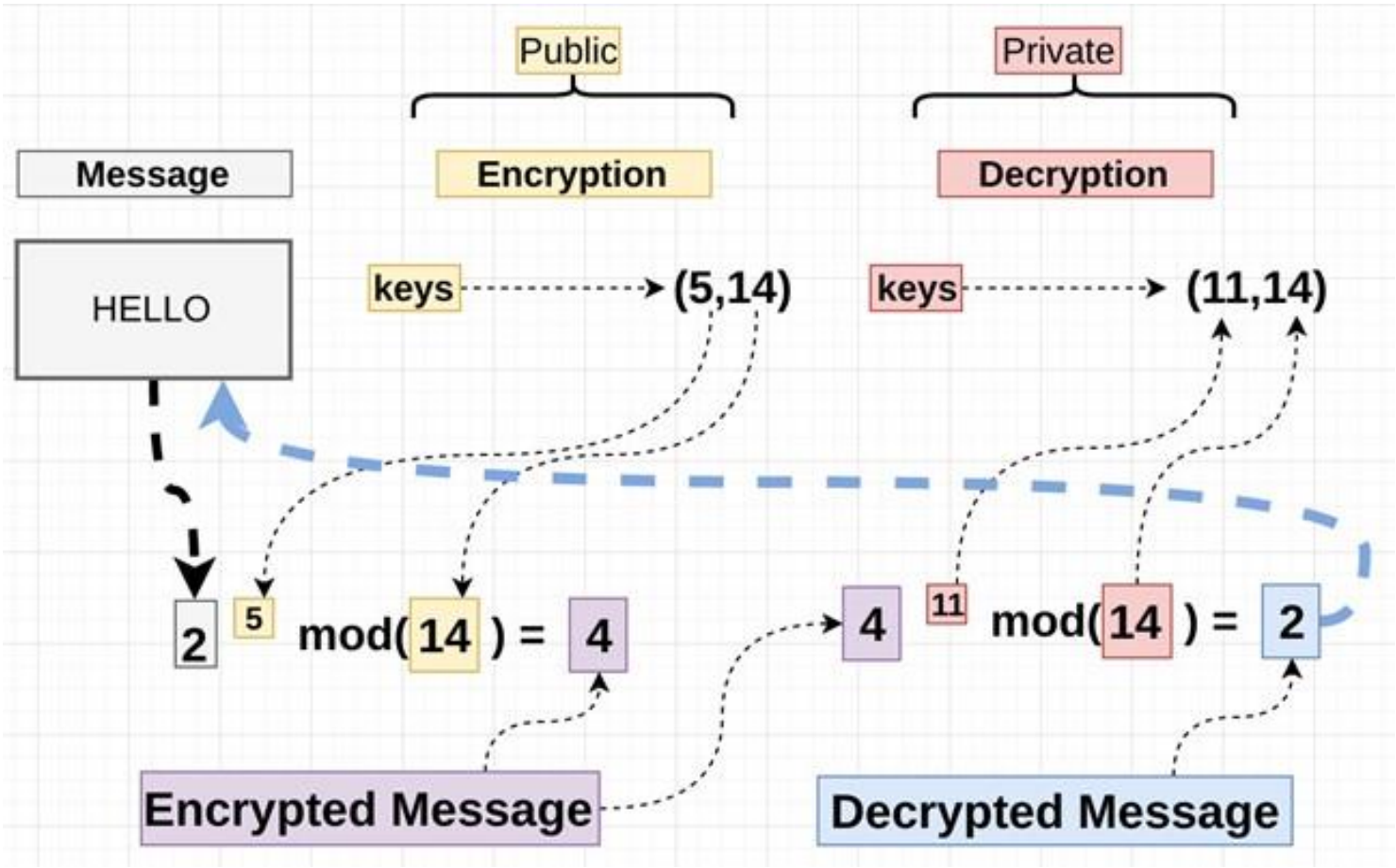
O RSA é um algoritmo relativamente lento e, por isso, é menos usado para cifrar diretamente os dados a serem transmitidos.

O RSA geralmente é usado em conjunto com algum algoritmo de chave simétrica, permitindo que a chave compartilhada possa ser transmitida de forma segura, e esta por sua vez, possa executar operações de cifrar-decifrar em massa a uma velocidade muito maior.



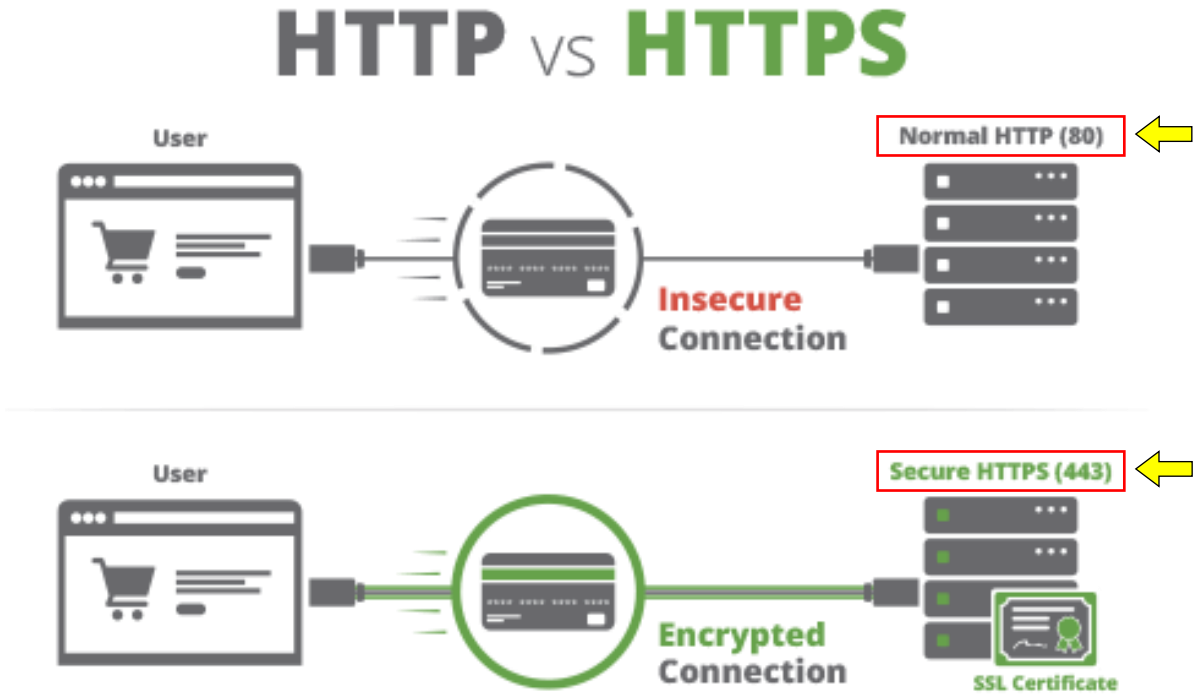
Fonte: www.wikipedia.org

RSA – exemplo


Public
Private
Message
Encryption
Decryption
HELLO
keys
(5,14)
keys
(11,14)
2
5
mod(14) = 4
4
11
mod(14) = 2
Encrypted Message
Decrypted Message

Secure Sockets Layer – protocolo

SSL (Secure Sockets Layer) é uma tecnologia de segurança padrão para estabelecer uma conexão criptografada entre um servidor e um cliente, que pode ser um servidor Web (site) e um navegador, ou um servidor de e-mail e um cliente de e-mail.



Fonte: www.digicert.com

Secure Sockets Layer – protocolo

O SSL permite que informações confidenciais, como números de cartão de crédito e credenciais de login sejam transmitidas com segurança, ao invés de serem enviados em texto simples.

O SSL é um protocolo de segurança que descreve como os algoritmos devem ser usados. Nesse caso, o protocolo SSL determina as variáveis da criptografia para o enlace e os dados que estão sendo transmitidos.

Todos os navegadores têm a capacidade de interagir com servidores da Web protegidos usando o protocolo SSL. No entanto, o navegador e o servidor precisam do que é chamado de Certificado SSL para poder estabelecer uma conexão segura.

Fonte: www.digicert.com

Secure Sockets Layer – certificado

O protocolo SSL requer autenticação entre o servidor e o cliente para proteger uma conexão, e para tal é necessário um certificado SSL.

O certificado SSL é emitido por um terceiro confiável, normalmente uma autoridade de certificação (AC).

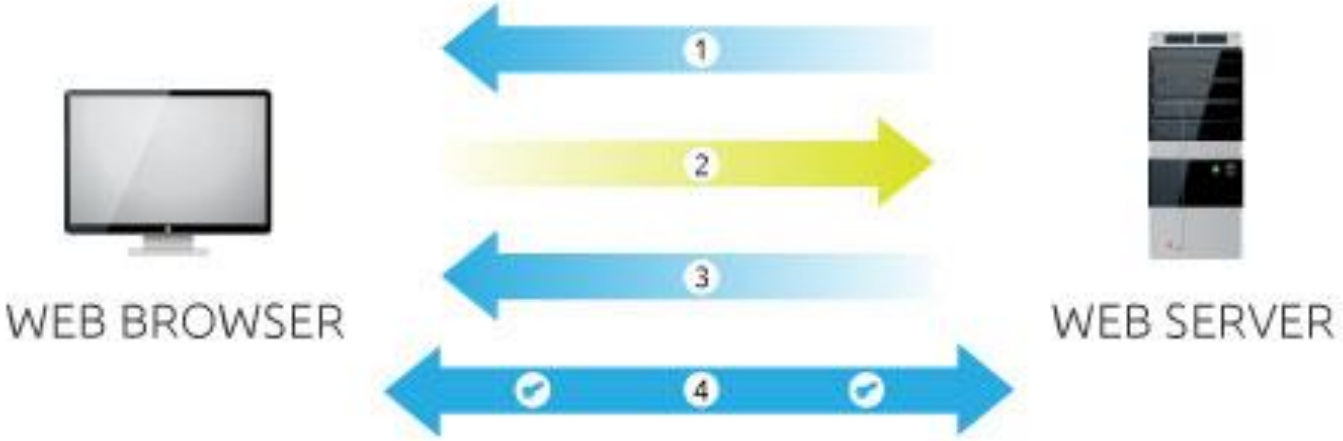
O certificado SSL vincula o domínio, o servidor ou o nome do servidor à identidade e localização de uma organização.

O certificado é instalado no servidor web da organização e fornece uma conexão segura entre o navegador do usuário e o servidor quando solicitado.

ATENÇÃO: protocolo SSL é diferente de certificado SSL!

Fonte: www.digicert.com

Secure Sockets Layer – aplicação

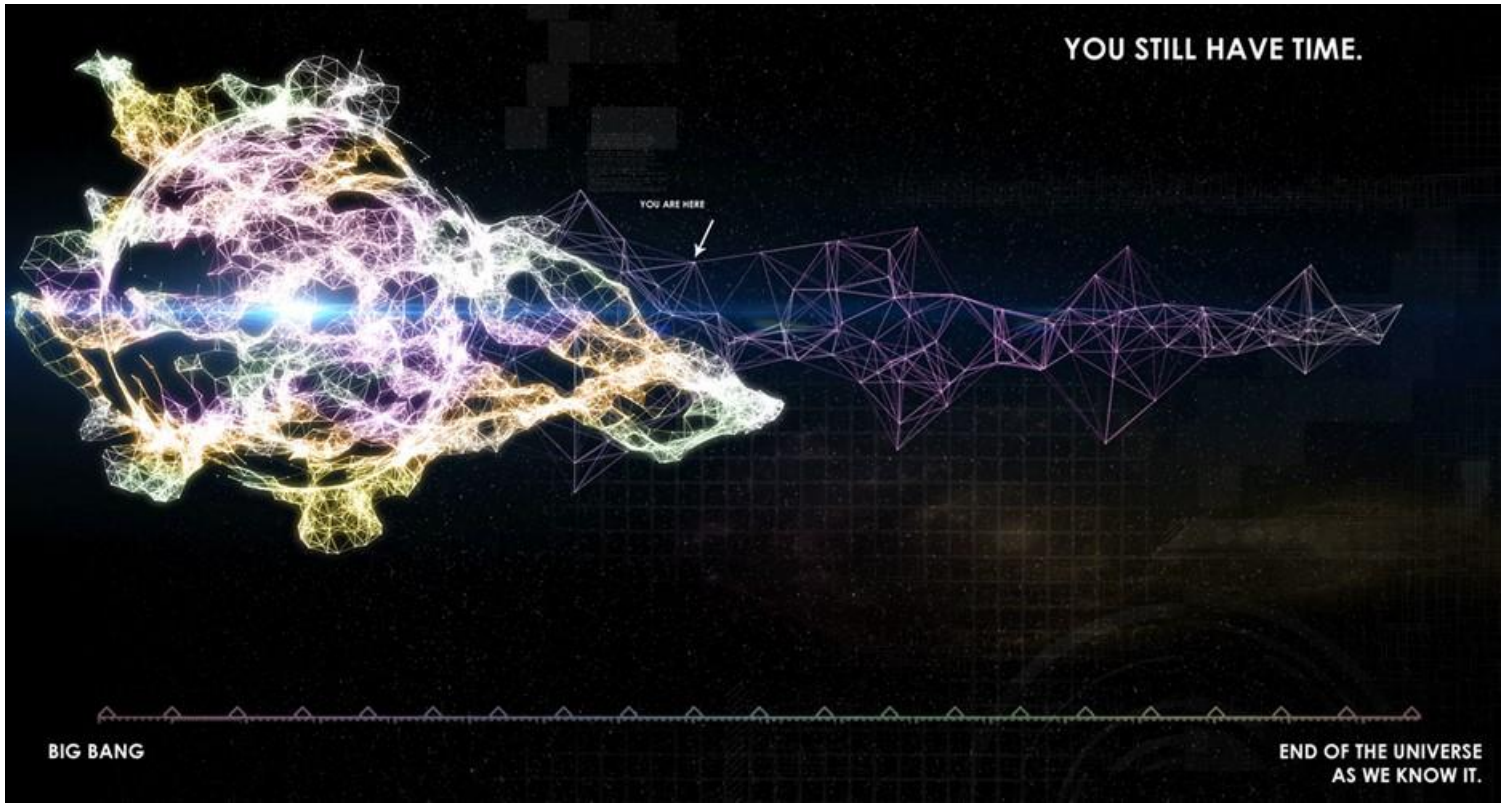


1. O Web Server envia uma cópia de sua chave pública assimétrica para o Web Browser;
2. O Web Browser cria uma chave de sessão simétrica e a criptografa com a chave pública assimétrica do Web Server e em seguida a envia para o servidor;
3. O Web Server decifra a chave de sessão criptografada usando sua chave privada assimétrica para obter a chave de sessão simétrica;
4. Web Server e Web Browser agora cifram e decifram todos os dados transmitidos com a chave de sessão simétrica. Isso permite um canal seguro porque somente o Web Server e o Web Browser conhecem a chave de sessão simétrica e esta é usada apenas para essa sessão. Se o Web Browser tivesse que se conectar ao mesmo Web Server no dia seguinte, uma nova chave de sessão seria criada.

Fonte: www.digicert.com

Secure Sockets Layer – segurança

Quanto tempo seria necessário para quebrar um certificado SSL de 2048 bits?*



Fonte: www.digicert.com

**Usando um desktop com processador AMD Opteron de 2.2 GHz com 2GB RAM.*

Transport Layer Security

SSL e TLS são protocolos criptográficos que fornecem autenticação e criptografia de dados entre servidores, máquinas e aplicativos que operam em uma rede.

O TLS é o sucessor do SSL, e ao longo dos anos novas versões destes protocolos foram lançadas para solucionar vulnerabilidades e oferecer suporte a conjuntos de algoritmos de codificação mais fortes e seguros.

O SSL foi originalmente desenvolvido pela Netscape e apareceu pela primeira vez em 1995 com o SSL 2.0, também conhecida como SSLv2. Em 1996 foi lançada a versão 3.0 (SSLv3), depois que várias vulnerabilidades foram encontradas na versão anterior.

O TLS foi introduzido em 1999 como uma nova versão do SSL e foi baseado no SSL 3.0. Atualmente o TLS está na versão 1.2.

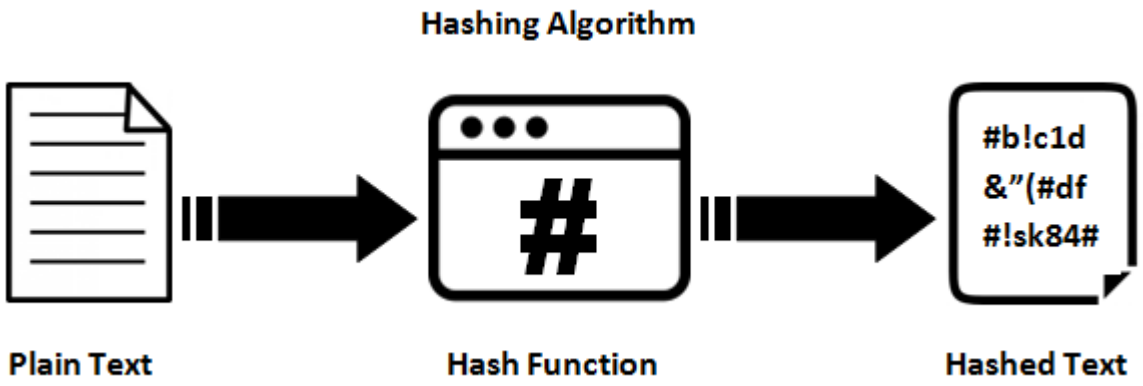
Nota: o SSL 1.0 nunca foi lançado ao público.

Fonte: www.globalsign.com

Função de resumo (*Hash*)

Uma função de resumo é um método criptográfico que, quando aplicado sobre uma informação, independente do tamanho que ela tenha, gera um resultado único e de tamanho fixo, chamado *hash*. Pode-se utilizar *hash* para:

- verificar a integridade de um arquivo obtido da Internet (alguns *sites*, além do arquivo em si, também disponibilizam o *hash* correspondente, para que se possa verificar se o arquivo foi corretamente transmitido e gravado);
- gerar assinaturas digitais.



Fonte: Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

Função de resumo (*Hash*)

Exemplos de métodos de *hash* são:

- SHA-1;
- SHA-256;
- MD5.

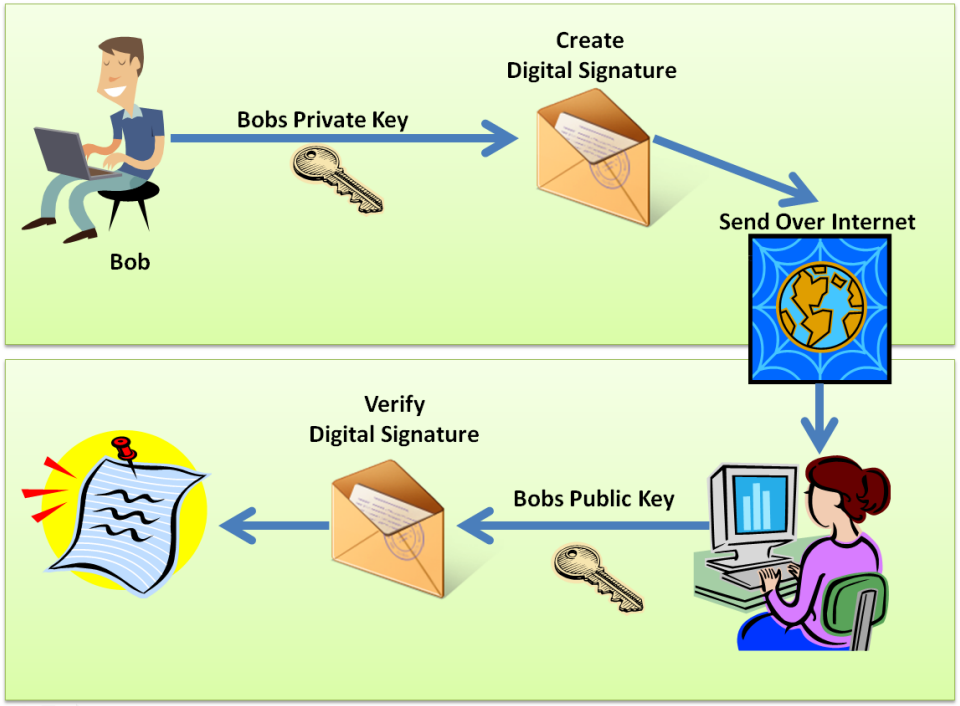
O *hash* é gerado de tal forma que não é possível realizar o processamento inverso para se obter a informação original e qualquer alteração na informação original produzirá um *hash* distinto.

Apesar de ser teoricamente possível que informações diferentes gerem *hashes* iguais, a probabilidade disto ocorrer é bastante baixa.

Fonte: Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

Assinatura digital

A assinatura digital permite comprovar a autenticidade e a integridade de uma informação, ou seja, que ela foi realmente gerada por quem diz ter feito isto e que ela não foi alterada.



Fonte: Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

Assinatura digital

A assinatura digital baseia-se no fato de que apenas o dono conhece a chave privada e que, se ela foi usada para codificar uma informação, então apenas seu dono poderia ter feito isto.

A verificação da assinatura é feita com o uso da chave pública, pois se o texto foi codificado com a chave privada, somente a chave pública correspondente pode decodificá-lo.

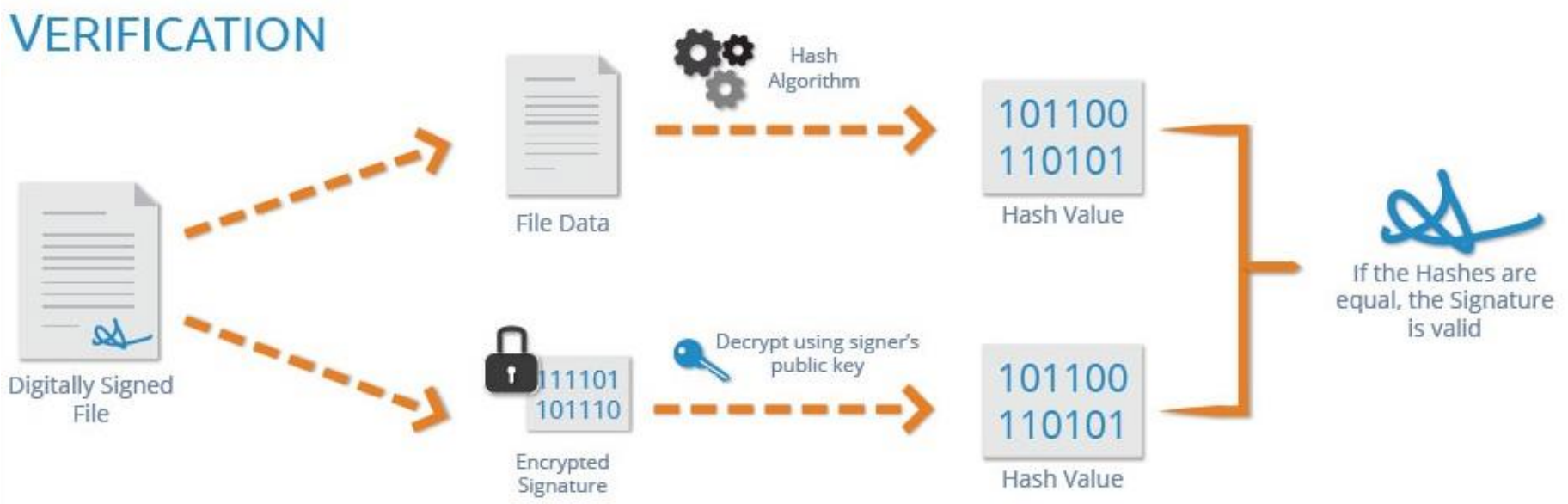
Para contornar a baixa eficiência característica da criptografia de chaves assimétricas, a codificação é feita sobre o *hash* e não sobre o conteúdo em si, pois é mais rápido codificar o *hash* (que possui tamanho fixo e reduzido) do que a informação toda.

A assinatura digital garante apenas que a informação foi de fato gerada pelo proprietário da chave privada.

Fonte: Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

Assinatura digital – assinando um documento

Assinatura digital – verificando um documento



Certificado digital

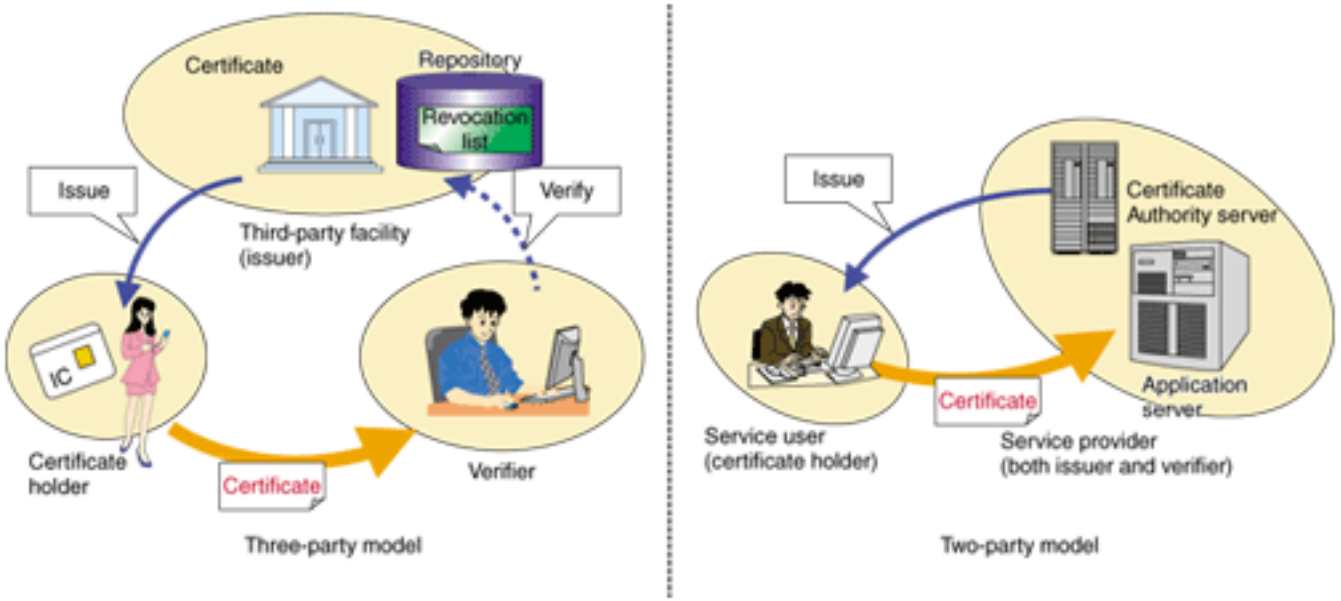
Na assinatura digital a chave púbica pode ser livremente divulgada, mas não há como comprovar a quem ela pertence de fato, e pode ocorrer em uma troca de mensagens da comunicação estar se dando com um impostor.

Um impostor pode criar uma chave pública falsa para um amigo seu e enviá-la para você ou disponibilizá-la em um repositório. Ao usá-la para codificar uma informação para o seu amigo, você estará, na verdade, codificando-a para o impostor, que possui a chave privada correspondente e conseguirá decodificar a mensagem. Uma das formas de impedir que isto ocorra é usando certificados digitais.

Fonte: Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

Certificado digital

O certificado digital é um registro eletrônico composto por um conjunto de dados que distingue uma entidade e associa a ela uma chave pública. Ele pode ser emitido para pessoas, empresas, equipamentos ou serviços na rede (por exemplo, um *site Web*) e pode ser homologado para diferentes usos, como confidencialidade e assinatura digital.



Fonte: Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

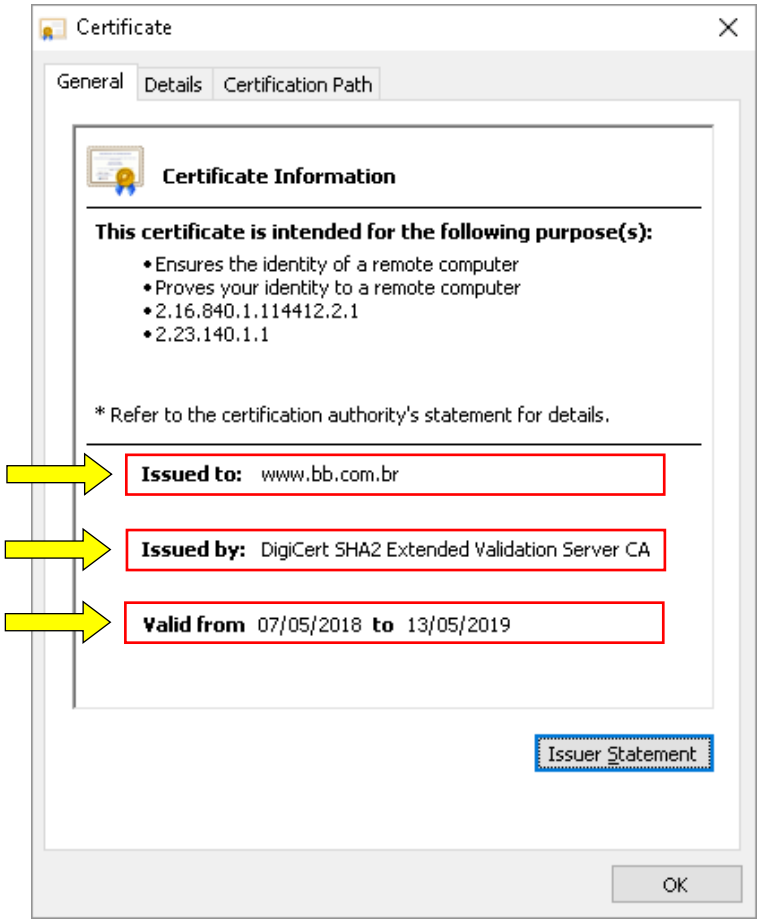
Certificado digital

Um certificado digital pode ser comparado a um documento de identidade, como o passaporte, por exemplo, no qual constam o dados pessoais do requerente e a identificação de quem o emitiu.

No caso do passaporte, a entidade responsável pela emissão e pela veracidade dos dados é a Polícia Federal.

No caso do certificado digital esta entidade é uma Autoridade Certificadora (AC).

O certificado deve conter os dados do emissor (Issued by), do requerente (Issued to) e a data de validade.

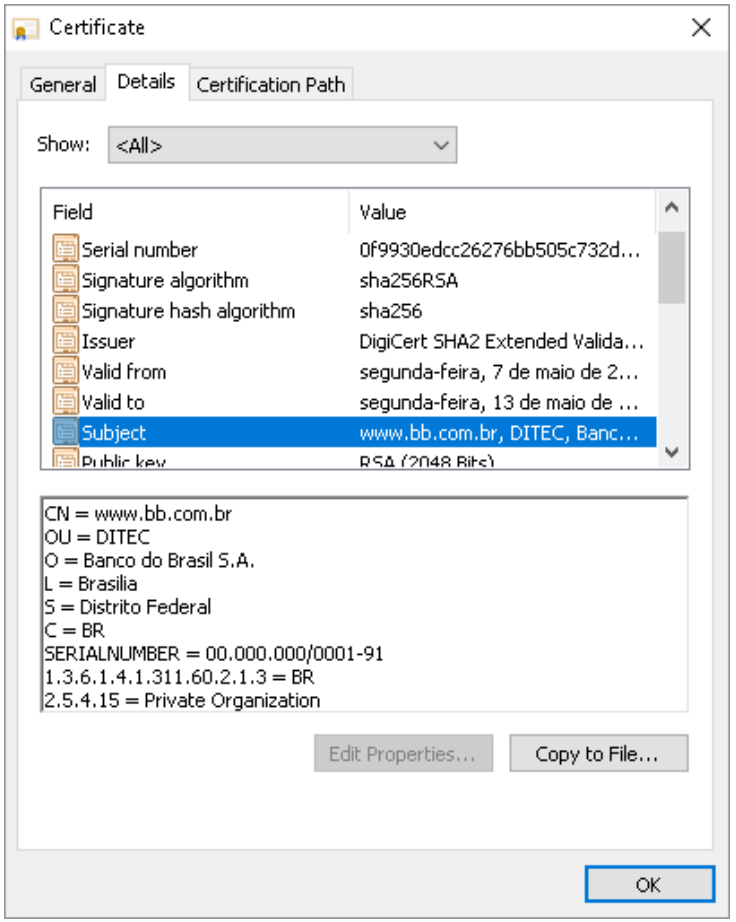


Fonte: Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

Certificado digital

De forma geral, os dados básicos que compõem um certificado digital são:

- versão e número de série do certificado;
- dados que identificam a AC que emitiu o certificado;
- dados que identificam o requerente do certificado (para quem ele foi emitido);
- chave pública do dono do certificado;
- validade do certificado (quando foi emitido e até quando é válido);
- assinatura digital da AC emissora e dados para verificação da assinatura.

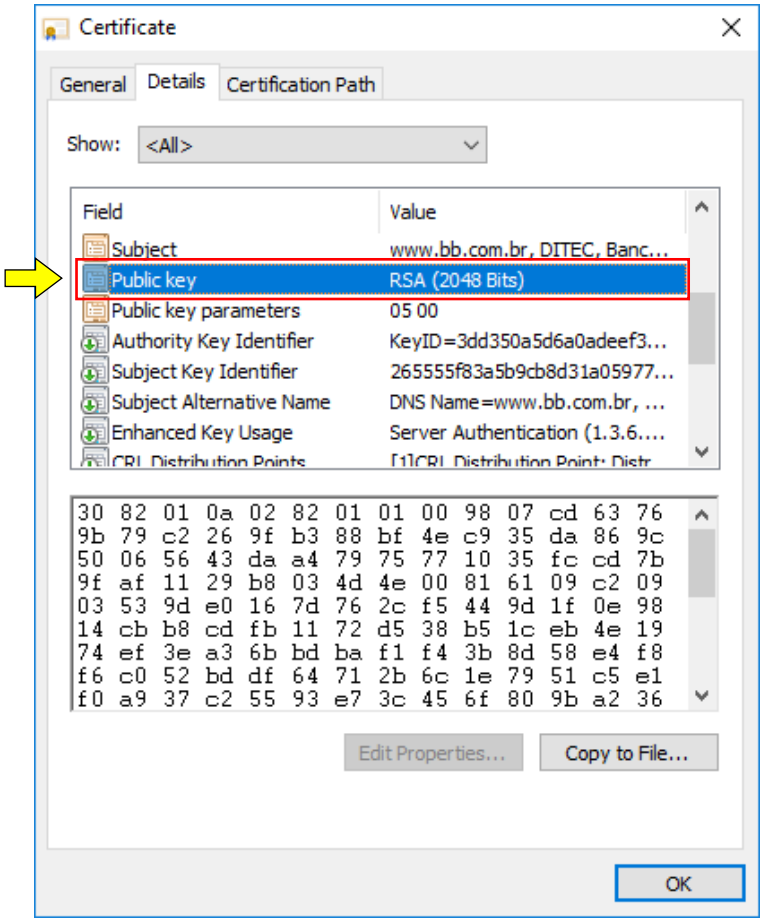


Fonte: Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

Certificado digital

Para verificar o algoritmo usado para gerar a chave pública e o tamanho da mesma em bits, deve-se olhar o campo Public Key.

No exemplo ao lado a chave foi gerada usando-se o algoritmo RSA e a mesma possui 2048 bits de tamanho.

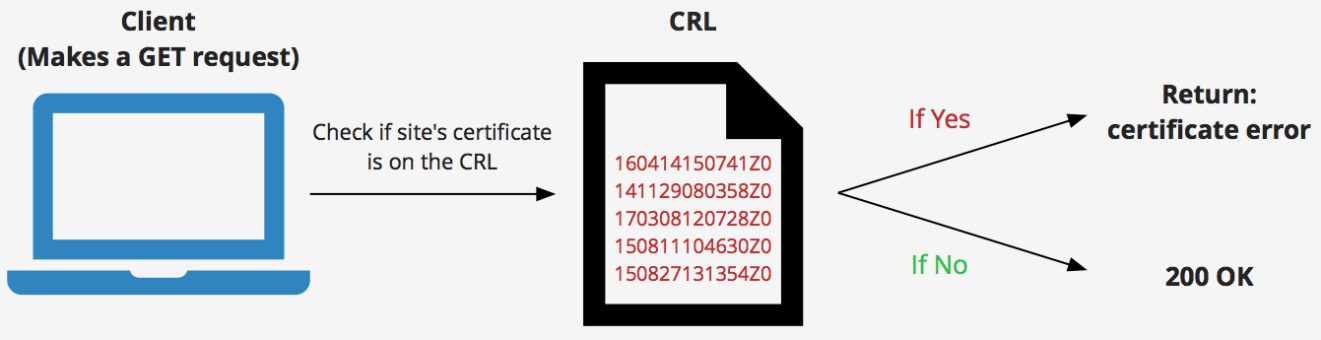


Certificado digital

Uma Autoridade Certificadora (AC ou CA, Certification Authority), além de emitir certificados, também é responsável por publicar informações sobre certificados que não são mais confiáveis.

Sempre que a AC descobre ou é informada que um certificado não é mais confiável, ela o inclui em uma "Lista de Certificados Revogados" (LCR ou CRL, Certificate Revocation List) para que os usuários possam tomar conhecimento.

A LCR é um arquivo eletrônico publicado periodicamente pela AC, contendo o número de série dos certificados que não são mais válidos e a data de revogação.



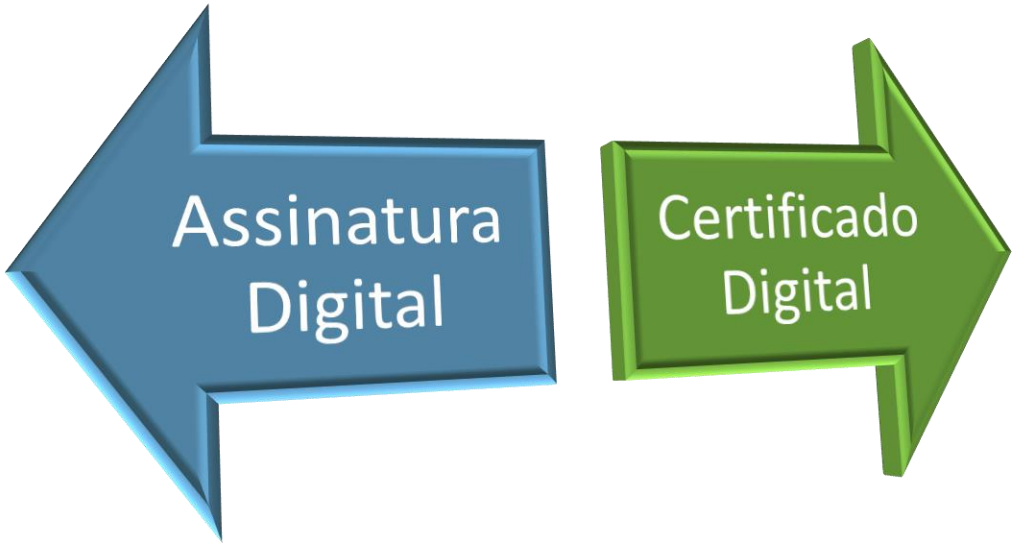
Fonte: Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

Certificado digital

Exemplo de site com certificado inválido

Assinatura digital vs Certificado digital

A assinatura digital garante apenas que a informação foi de fato gerada pelo proprietário da chave privada.



O certificado digital serve para verificar quem é o proprietário da chave privada usada, mas é necessário confiar em um terceiro (AC) que ateste tal propriedade.

Módulo 10

Infraestrutura de chaves públicas

Public Key Infrastructure

Com a evolução da criptografia de chaves públicas e o conceito da existência de uma chave pública que pode ser distribuída livremente, surgiram novas necessidades e questões a serem tratadas.

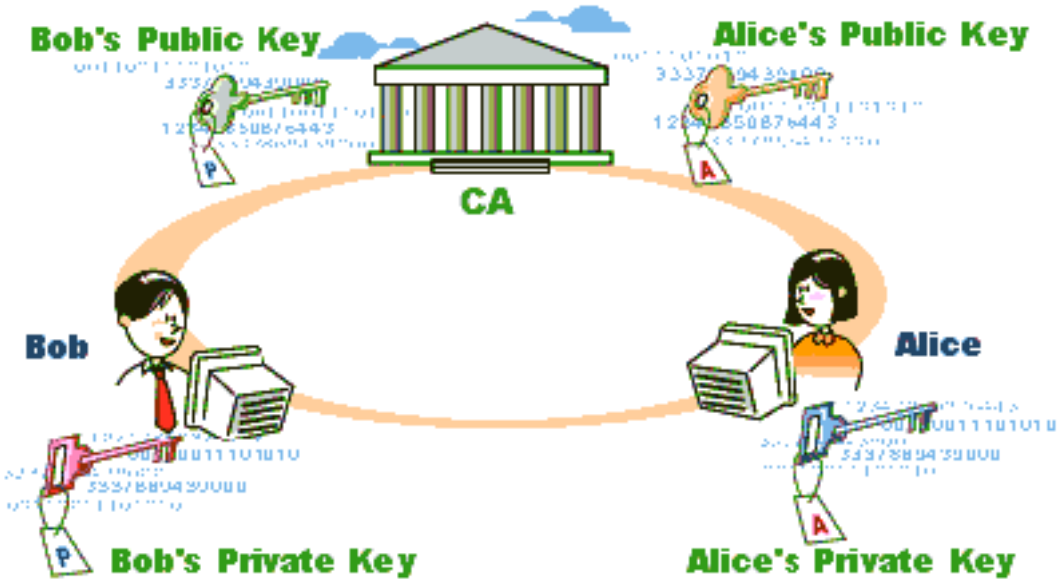
Entre elas merece destaque a questão de como associar uma chave pública ao seu autêntico proprietário. Esta associação pode ser feita através dos certificados digitais.

No entanto, também se faz necessária uma entidade confiável para atestar a ligação entre o proprietário e/ou responsável pela chave e a sua respectiva chave pública.

Fonte: Escola Superior de Redes RNP

Public Key Infrastructure

De acordo com a especificação X.509, foi criado o conceito de uma entidade chamada de Autoridade Certificadora (AC), que é responsável pela identificação do usuário e por atestar que ele possui a chave privada correspondente à chave pública.



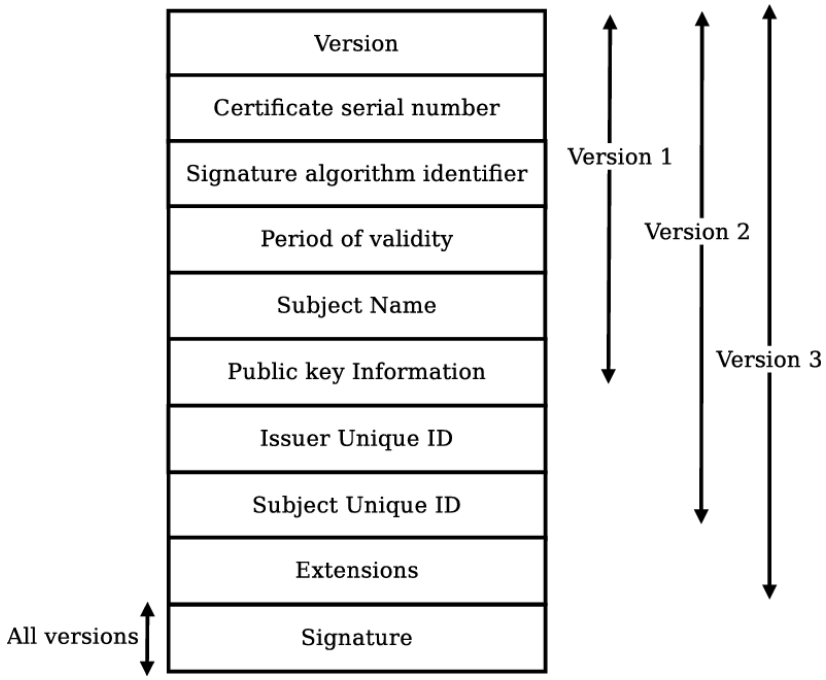
Fonte: Escola Superior de Redes RNP

Public Key Infrastructure

O processo de identificar o usuário e atestar que ele possui a chave privada correspondente à chave pública é realizado através da assinatura de um documento pela AC, que contém dados de identificação do usuário, sua chave pública e outros atributos necessários.

Este documento é chamado de Certificado Digital X.509 e representa o mais básico elemento de uma PKI (ou ICP, Infraestrutura de Chaves Públicas).

O padrão X.509 foi definido pela ITU-T (International Telecommunication Union – Telecommunication Standardization Sector) e especifica, entre outras coisas, o formato dos certificados digitais.



Formato do certificado digital X.509

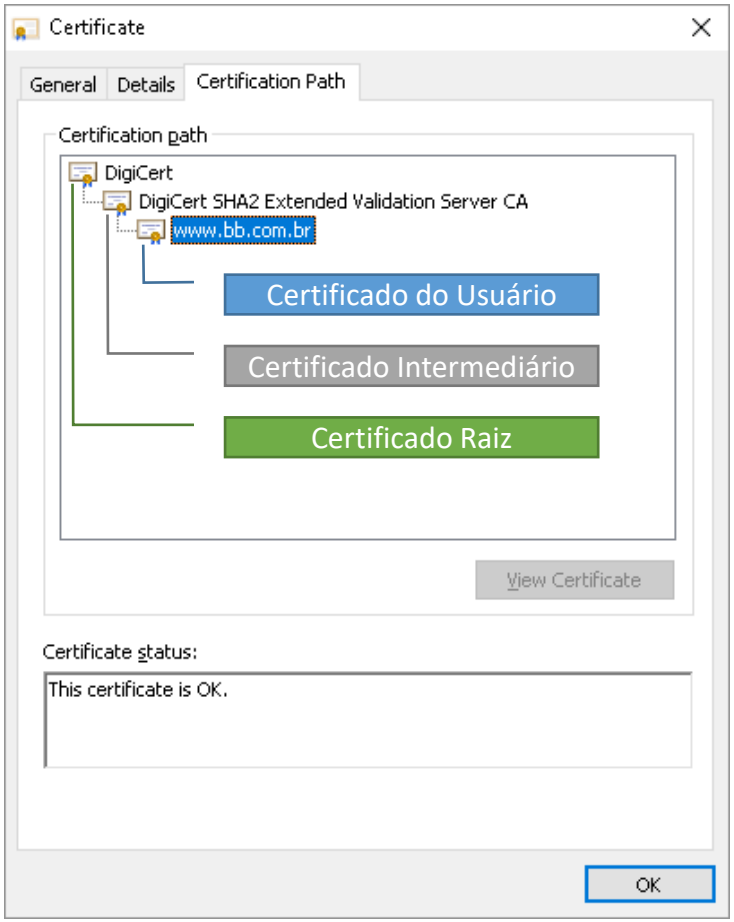
Fonte: Escola Superior de Redes RNP

Public Key Infrastructure

O certificado digital de uma AC é emitido, geralmente, por outra AC, estabelecendo uma hierarquia conhecida como “cadeia de certificados” ou “caminho de certificação”.

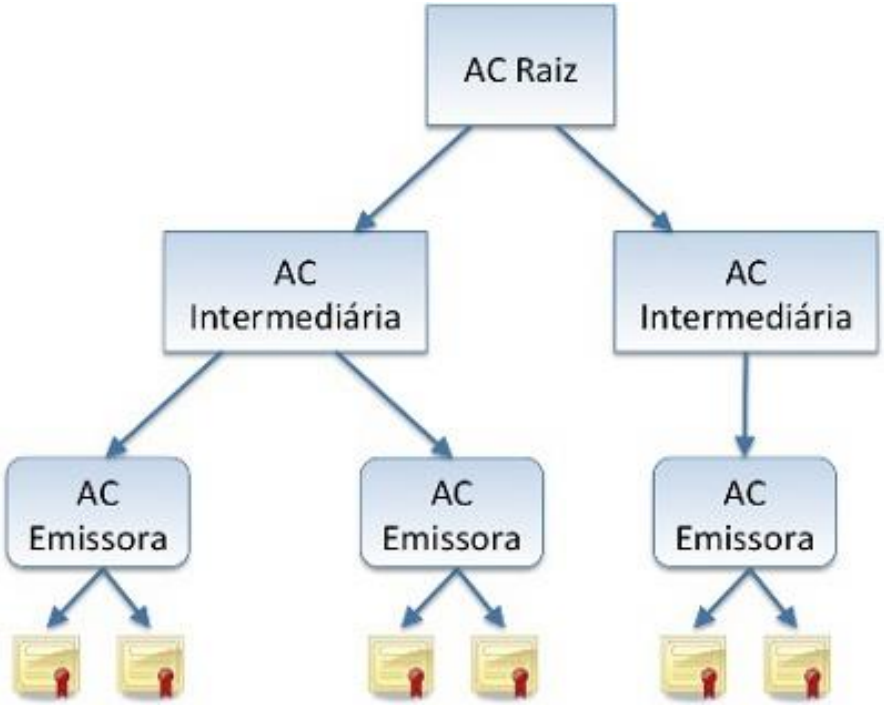
A AC raiz, primeira autoridade da cadeia, é a âncora de confiança para toda a hierarquia e, por não existir outra AC acima dela, possui um certificado autoassinado.

Um certificado autoassinado é aquele no qual o dono e o emissor são a mesma entidade.



Fonte: Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

Public Key Infrastructure



Hierarquia de Entidades Certificadoras

Fonte: Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

Public Key Infrastructure

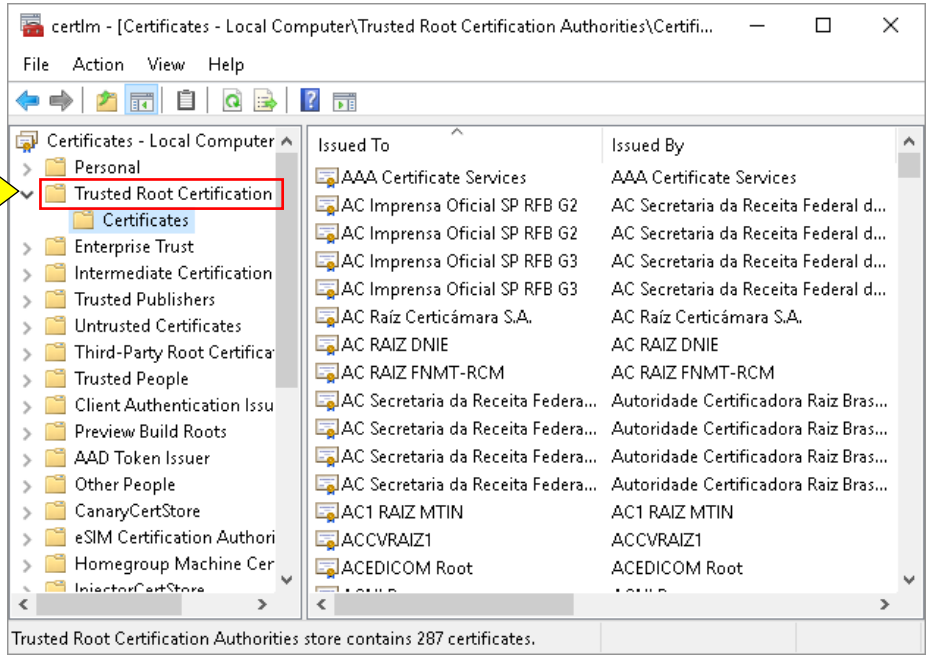
Os certificados das ACs raízes publicamente reconhecidas já vêm inclusos, por padrão, em grande parte dos sistemas operacionais e navegadores e são atualizados juntamente com os próprios sistemas.

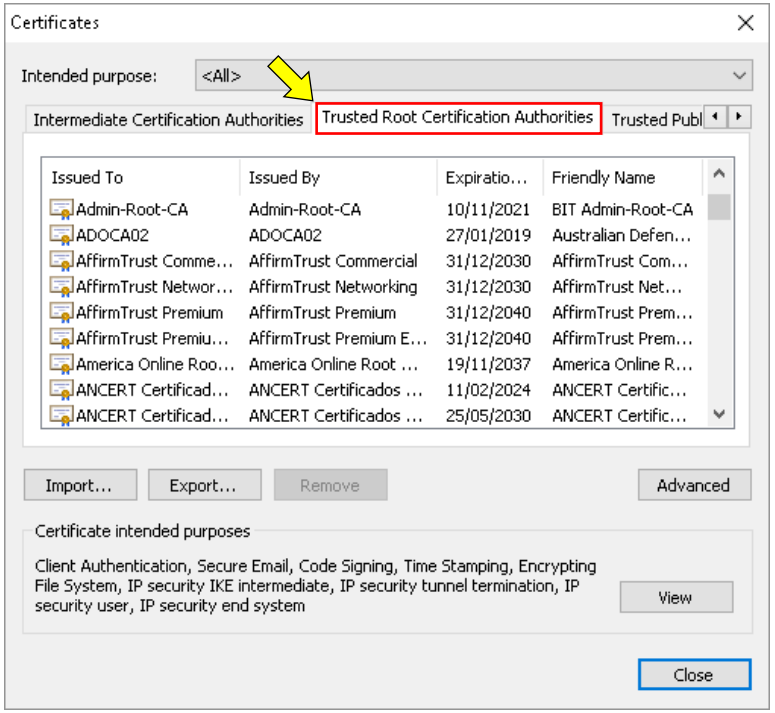
Alguns exemplos de atualizações realizadas na base de certificados dos navegadores são:

- inclusão de novas ACs;
- renovação de certificados vencidos;
- exclusão de ACs não mais confiáveis.

Fonte: Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

Public Key Infrastructure





ACs reconhecidos pelo sistema operacional Windows 10*

ACs reconhecidos pelo navegador Google Chrome*

*As ACs podem ser gerenciadas (incluídas, alteradas ou removidas) pelo administrador do sistema.

Public Key Infrastructure
Autoridade Certificadora

A Autoridade Certificadora (AC) é composta por hardware, software e pessoas que a operam. É o elemento de uma ICP responsável pela emissão de certificados, emissão de LCRs, gerenciamento e publicação das informações sobre certificados revogados, além de ser capaz de delegar determinadas funções a outras entidades.

Fonte: Escola Superior de Redes RNP

Public Key Infrastructure
Autoridade Certificadora

Ao emitir um certificado, uma AC assegura que a entidade requisitante detém a chave privada correspondente à chave pública contida no certificado.

Os certificados emitidos podem ser para outras ACs (conhecidas como ACs intermediárias), para entidades finais ou para ambos.

Quando emite LCRs, uma AC gera uma lista assinada contendo informações sobre os certificados revogados, como a data e o motivo da revogação.

De maneira semelhante ao certificado, quando uma AC assina sua LCR, ela atesta seu conhecimento e a autenticidade do conteúdo da lista.

Fonte: Escola Superior de Redes RNP

Public Key Infrastructure
Autoridade Certificadora

Uma infraestrutura de chaves públicas pode ser constituída por uma única AC, porém em muitos casos faz-se necessário que determinadas tarefas sejam delegadas a outras entidades a fim de minimizar a carga de tarefas sobre a AC.

Por exemplo, uma AC pode delegar a outra AC, denominada AC intermediária, a emissão de certificados em seu nome, ou então delegar a emissão da LCR a outra AC.

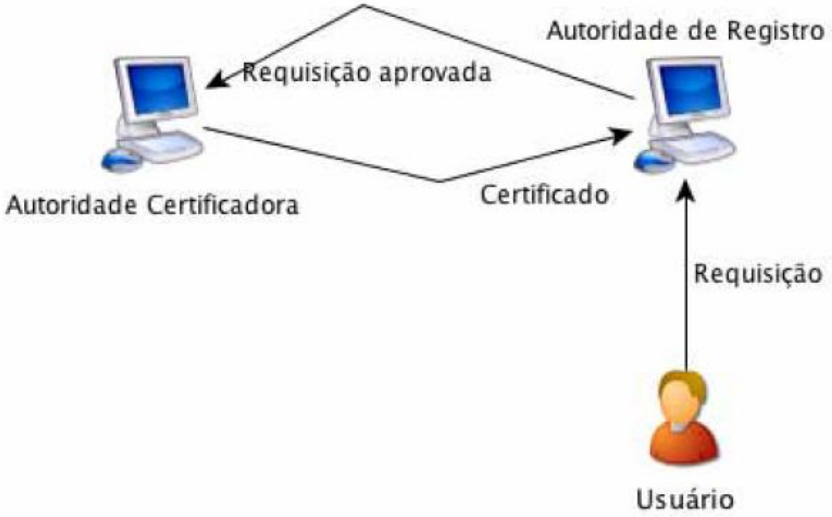
Outra delegação de tarefa bastante comum em uma AC é a de delegar o processo de identificação dos usuários para uma entidade chamada Autoridade de Registro (AR).

Fonte: Escola Superior de Redes RNP

Public Key Infrastructure
Autoridade de Registro

A Autoridade de Registro (AR) é uma entidade composta por software, hardware e operadores para os quais a AC delega a tarefa de verificar o conteúdo de requisições de certificados. Uma AC pode delegar a tarefa de verificação de informações para várias ARs, que podem desempenhar seu papel para várias ACs.

A existência desta entidade em uma ICP faz-se necessária de acordo com a abrangência que uma AC pode ter, seja ela por sua distribuição geográfica, ou por um elevado número de usuários.



Fonte: Escola Superior de Redes RNP

Public Key Infrastructure
Repositório

O Repositório de Certificados Digitais também atua por delegação da AC, e é normalmente composto por software e hardware com o objetivo de publicar os certificados digitais e listas de certificados revogados atuais emitidos por uma ou mais ACs.

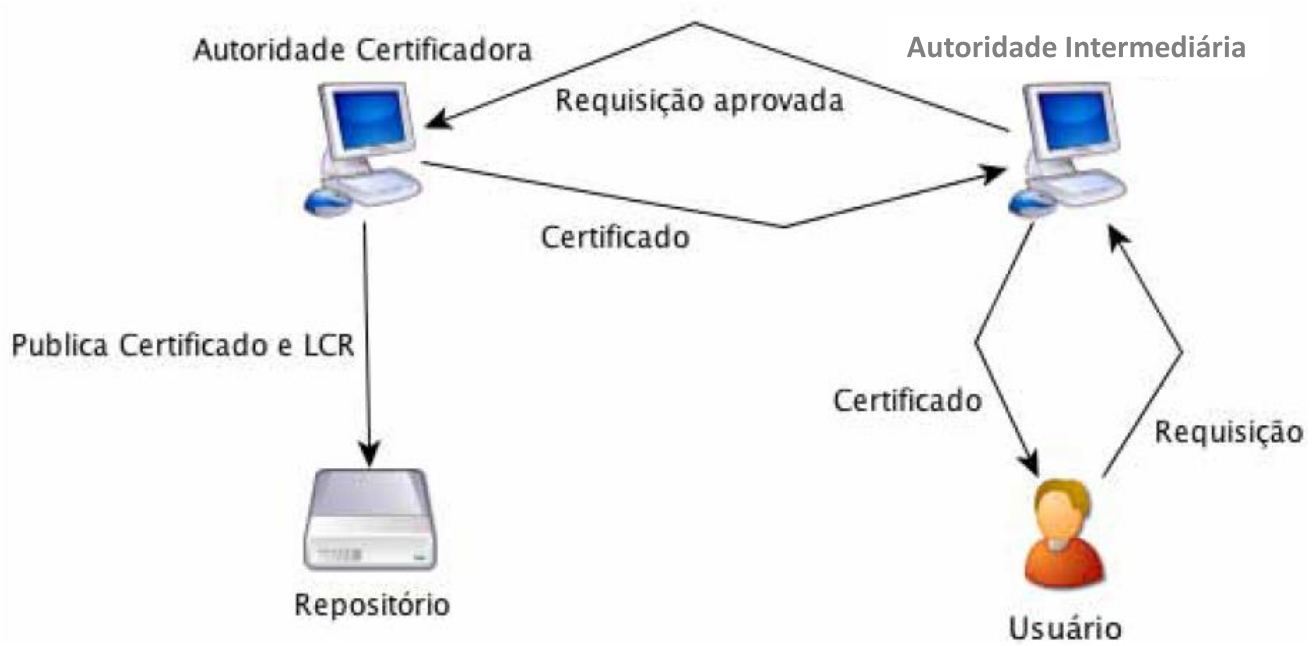
Os dados disponibilizados e armazenados pelo Repositório de Certificados Digitais são assinados pela AC representada por ele, garantindo sua integridade e sua autenticidade e tornando-o imune a ataques de substituição e fabricação.

O Repositório de Certificados Digitais é uma parte da ICP que precisa estar sempre disponível, e por isso necessita de medidas de segurança que garantam a sua disponibilidade.

Fonte: Escola Superior de Redes RNP

Public Key Infrastructure
ACs Intermediárias

Uma AC pode delegar a responsabilidade de emissão de certificados para uma ou mais ACs Intermediárias.



Fonte: Escola Superior de Redes RNP

Public Key Infrastructure
ACs Intermediárias

Os motivos pelos quais uma AC pode fazer isto são:

- Redução da carga de trabalho sobre uma AC, fazendo com que a AC Raiz tenha que emitir um número menor de certificados, dividindo esta tarefa com outras Acs;
- Facilitar o crescimento de toda a estrutura da AC;
- Aumentar a abrangência (se necessário), já que com mais ACs é possível distribuir melhor a localização e o escopo das emissões de certificados digitais;
- Melhorar a capacidade de tolerância a erros, uma vez que se uma AC Intermediária tiver problemas, apenas o que está abaixo desta AC será comprometido. Se houvesse apenas a AC Raiz, a estrutura toda seria comprometida.

Se a AC Raiz autorizar, uma AC Intermediária pode delegar a tarefa de emissão para outras ACs abaixo dela. Além disso, pode limitar o número de ACs abaixo dela através do uso de uma extensão específica para este fim.

Fonte: Escola Superior de Redes RNP

Para saber mais...

… leia a Cartilha de Segurança para Internet do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

... leia a apostila Introdução a Infraestrutura de Chaves Públicas e Aplicações, da Escola Superior de Redes RNP

Módulo 11

Privacidade

Introdução

Privacidade é o direito à reserva de informações pessoais e da própria vida pessoal.

A origem do termo privacidade no campo jurídico remete ao “right to privacy”.

A privacidade (privacy) pode ser definida como o direito de estar só ou ser deixado só (“right to be let alone”).

Assim, entende-se que a privacidade pode sofrer ataques, podendo gerar desgastes e dores muito maiores que uma injúria corporal.

Fonte: Enciclopédia Jurídica da PUC SP

O que é LGPD?

A Lei Federal nº 13.709, promulgada em 14 de agosto de 2018, instituiu a Lei Geral de Proteção de Dados Pessoais, também conhecida pelo seu acrônimo LGPD.

Seu objetivo é garantir a proteção da privacidade e da intimidade das pessoas, que estão cada vez mais expostas ao significativo aumento do processamento de dados e do compartilhamento de informações pessoais dos indivíduos.

Fonte: Lei Federal nº 13.709 de 14/08/2018

O que é LGPD?

A lei também visa regulamentar o tratamento de dados pessoais dos indivíduos, seja em meios físicos ou digitais, para garantir os direitos fundamentais relacionados à liberdade, privacidade e intimidade das pessoas, bem como assegurar aos seus titulares a máxima transparência sobre qualquer forma de utilização de seus dados.

Vigência

- A partir de 18 de setembro de 2020;
- Sanções administrativas a partir de 1º de agosto de 2021.

Fonte: Lei Federal nº 13.709 de 14/08/2018

E se as farmácias compartilhassem seus dados pessoais com as seguradoras?

As farmácias coletam dados de seus clientes para cadastrá-los em seus programas de fidelidade, com a justificativa de oferecer descontos e o acesso a promoções.

As seguradoras poderiam, com base no histórico de compras dos indivíduos, estabelecer níveis de preços mais altos para a contratação de determinados planos de saúde, ou simplesmente negar a cobertura.

Histórico

ANO	EVENTO
1948	Declaração Universal dos Direitos Humanos
1950	Convenção Europeia sobre Direitos Humanos
1981	Convenção para Proteção de Indivíduos relativamente ao Processamento Automático de Dados Pessoais
1995	Diretiva 95/46/EC – Diretiva de Privacidade (válida até 25/05/2018)
2002	Carta dos Direitos Fundamentais da União Europeia
2016	Regulamento Geral de Proteção de Dados – GDPR (válida a partir de 25/05/2018)

Fonte: Privacy & Data Protection, Exin

Histórico

"Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei."

Artigo 12 da Declaração Universal dos Direitos Humanos, 1948

Fonte: Privacy & Data Protection, Exin

Histórico

Respeito à vida privada e familiar

Toda pessoa tem o direito à sua vida privada e familiar, sua casa e sua correspondência.

Artigo 7 da Carta dos Direitos Fundamentais da União Europeia, 2002

Fonte: Privacy & Data Protection, Exin

Histórico

Proteção de dados pessoais

1. Toda pessoa tem direito à proteção dos dados pessoais que lhe digam respeito.

2. Esses dados devem ser tratados de forma justa para fins específicos e com base no consentimento da pessoa em causa ou em qualquer outra base legítima estabelecida por lei. Todos têm o direito de acessar os dados coletados sobre ele e o direito de retificá-los.

3. O cumprimento destas regras está sujeito ao controle de uma autoridade independente.

Artigo 8 da Carta dos Direitos Fundamentais da União Europeia, 2002

Fonte: Privacy & Data Protection, Exin

Histórico

A fim de se estabelecer um instrumento abrangente que tivesse validade em todos os países membros da União Europeia, em 2016 foi promulgado o Regulamento Geral de Proteção de Dados (General Data Protection Regulation), que visa o desenvolvimento do comércio internacional e a proteção da privacidade no intercâmbio de dados pessoais.

Fonte: Privacy & Data Protection, Exin

Histórico

A GDPR estabelece que o tratamento de dados de cidadãos de países membros da União Europeia só poderá se dar em outros países que também possuam legislação própria de proteção da privacidade.

A fim de manter as relações comerciais com a União Europeia, o Congresso Nacional se articulou para criar a LGPD, que tem como órgão máximo no território nacional a Autoridade Nacional de Proteção de Dados.

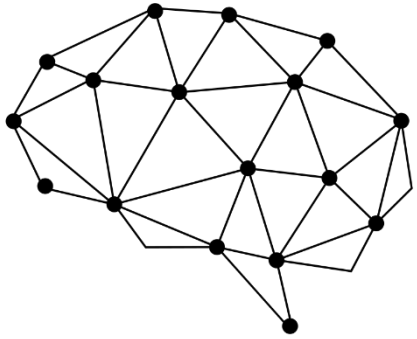
Exemplo de violação da privacidade
Caso Facebook/Cambridge Analytica

O documentário The Great Hack (Privacidade Hackeada), conta a história do escândalo que envolveu o Facebook, acusado de negligência por permitir que a empresa Cambridge Analytica coletasse dados de 87 milhões de usuários sem autorização, provocando um abalo na confiança da empresa, que virou alvo de investigações em diferentes países.

Fonte: WISNIK, Guilherme. Privacidade Hackeada alerta para manipulação de dados obtidos no mundo virtual. Jornal da USP

Exemplo de violação da privacidade
Caso Facebook/Cambridge Analytica

Com os dados coletados, a Cambridge Analytica, uma "empresa de comunicação orientada por dados", utilizou as informações "classificadas" dos usuários da rede social para influenciá-los em campanhas políticas, especialmente a do presidente Donald Trump à Presidência dos Estados Unidos, em 2016.



Cambridge Analytica

Fonte: WISNIK, Guilherme. Privacidade Hackeada alerta para manipulação de dados obtidos no mundo virtual. Jornal da USP

LGPD – Dado pessoal – Art. 15

Dado pessoal é a informação relacionada a pessoa natural identificada ou identificável.

Fonte: Lei Federal nº 13.709 de 14/08/2018

LGPD – Dado pessoal sensível – Art. 5

Dado pessoal sensível é todo dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Fonte: Lei Federal nº 13.709 de 14/08/2018

LGPD – Titular – Art. 5

O titular é a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

Fonte: Lei Federal nº 13.709 de 14/08/2018

LGPD – Tratamento – Art. 5

Tratamento é toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Fonte: Lei Federal nº 13.709 de 14/08/2018

LGPD – Princípios de tratamento – Art. 6

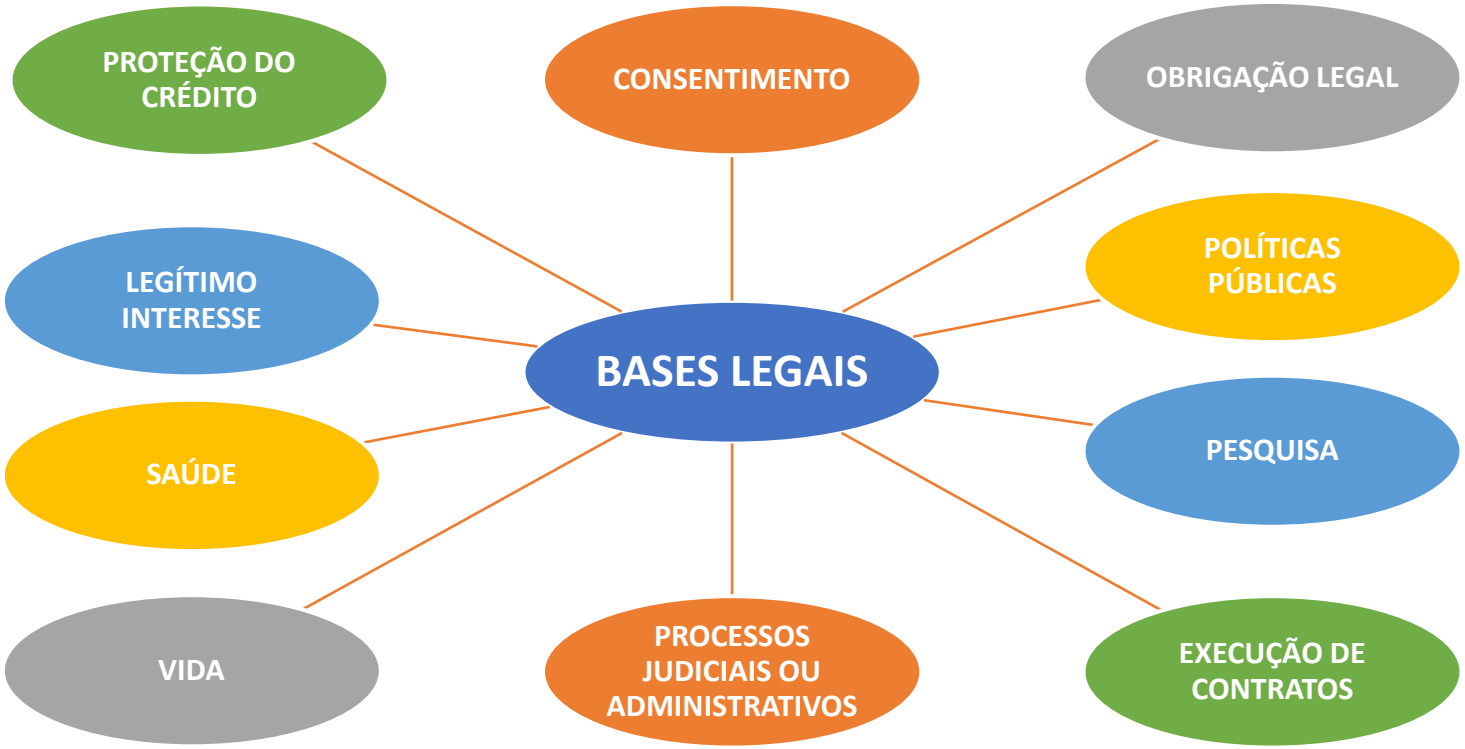
As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

FINALIDADE	ADEQUAÇÃO	NECESSIDADE	LIVRE ACESSO	QUALIDADE DOS DADOS
TRANSPARÊNCIA	SEGURANÇA	PREVENÇÃO	NÃO DISCRIMINAÇÃO	RESPONSABILIZAÇÃO

Fonte: Lei Federal nº 13.709 de 14/08/2018

LGPD – Requisitos para tratamento – Art. 7

O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:



Fonte: Lei Federal nº 13.709 de 14/08/2018

LGPD – Agentes de tratamento – Art. 5

Os agentes de tratamento são o controlador, a quem competem as decisões referentes ao tratamento de dados pessoais, e o operador, que realiza o tratamento de dados pessoais em nome do controlador.

O encarregado é a pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Fonte: Lei Federal nº 13.709 de 14/08/2018; FENABRAVE, Guia Melhores Práticas para Aplicação da LGPD.

Privacidade vs Segurança

PRIVACIDADE DE DADOS	≠	SEGURANÇA DE DADOS
A privacidade de dados se concentra nos direitos dos indivíduos, na finalidade de coleta e processamento de dados, nas preferências de privacidade e na maneira como as organizações controlam os dados pessoais dos titulares de dados. Ela se concentra em como coletar, processar, compartilhar, arquivar e excluir os dados de acordo com a lei.		A segurança de dados diz respeito aos meios de proteção que uma organização está adotando para impedir que terceiros não autorizados acessem os seus dados. Ela se concentra na proteção de dados contra ataques maliciosos e impede a exploração de dados (violação de dados ou ciberataque). Inclui controles de acesso, criptografia, segurança de rede, etc.

Fonte: Fundamentos da Lei Geral de Proteção de Dados, CertiProf.

LGPD e ISO 27000

CATEGORIA	DESCRIÇÃO DA CATEGORIA (ISO/IEC 27002)	LGPD
A.5	Políticas de segurança da informação	Art. 50
A.6	Organização da segurança da informação	Art. 5 e Art. 23
A.8	Gestão de ativos	Art. 5 e Art. 6
A.9	Controle de acesso	Art. 46
A.13	Segurança nas comunicações	Art. 33
A.14	Aquisição, desenvolvimento e manutenção de sistemas	Art. 49
A.16	Gestão de incidentes de segurança da informação	Art. 48
A.18	Conformidade	Art. 37

Fonte: SANTANA, W. R.; et. al. Aplicação da norma NBR ISO/IEC 27002 para atendimento do Marco Civil da Internet e da LGPD. CONTECSI USP – 17th International Conference on Information Systems and Technology Management, São Paulo, 2020

Para saber mais...

… leia o artigo SANTANA, W. R.; et. al. **Aplicação da norma NBR ISO/IEC 27002 para atendimento do Marco Civil da Internet e da LGPD**. CONTECSI USP – 17th International Conference on Information Systems and Technology Management, São Paulo, 2020

Módulo 12

Oportunidades no mercado de Segurança da Informação

Introdução

A expansão do mercado de TI no Brasil já não é uma surpresa para os mais diferentes segmentos da sociedade. O aumento da imersão no mundo digital, ainda que carregado de melhorias no cotidiano das pessoas, despertou também a atenção de sujeitos mal-intencionados que viram no mundo cibernético um espaço para explorar vulnerabilidades e propagar ameaças maliciosas.

Em janeiro de 2021, o World Economic Forum's Global Risks Report elencou os ataques cibernéticos como um dos riscos globais mais impactantes dos próximos anos. A incidência de organizações e empresas vítimas de ataques cibernéticos também é alvo constante de estudos por toda parte do globo.

Em 2019, o Ponemon Institute divulgou que 90% das empresas que lidam com os setores básicos da infraestrutura de um país – como energia, saúde, indústria, manufatura e transporte – já sofreram ao menos um ataque cibernético.

Esse cenário apenas reforça a necessidade de profissionais especializados e qualificados para atuarem no mercado de cibersegurança.

Fonte: Guia Completo para Entrada no Mundo da Cibersegurança, CECyber

Introdução

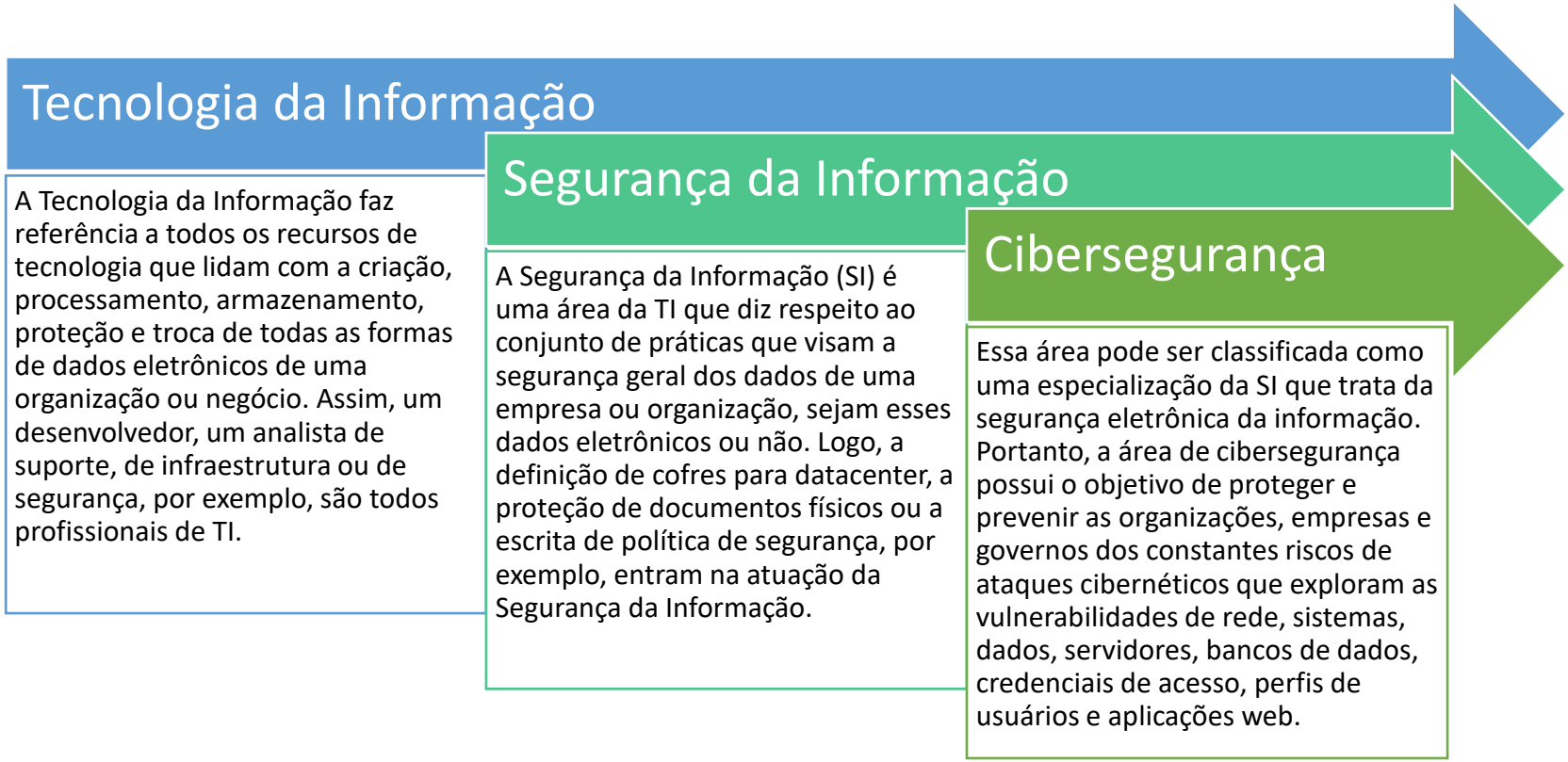
A pesquisa do Cybersecurity Workforce Study (ISC)², de 2019, constatou que a maior parte dos especialistas em segurança cibernética e TI são satisfeitos e otimistas com o futuro da profissão. Contudo, o mesmo trabalho demonstrou que a quantidade de tais profissionais de segurança não atinge os números necessários para que as organizações se mantenham seguras. Em outras palavras, não há profissionais suficientemente especializados para preencherem as demandas impostas pelo mundo cibernético.

Soma-se ainda o fato de que, com a pandemia da COVID-19, as empresas passaram a captar ainda mais dados de seus clientes, e, por consequência, as atenções dos invasores cibernéticos ficaram ainda maiores.

No Brasil, a falta de profissionais técnicos capacitados para atuarem em uma área em que a especialização é mandatória, como é o caso da cibersegurança, é ainda maior.

Fonte: Guia Completo para Entrada no Mundo da Cibersegurança, CECyber

Tecnologia da Informação vs Cibersegurança



Fonte: Guia Completo para Entrada no Mundo da Cibersegurança, CECyber

Tecnologia da Informação vs Cibersegurança

Em 2018, a International Telecommunication Union (ITU) classificou a cibersegurança como “a coleção de ferramentas, políticas, diretrizes, abordagens de gestão de risco, ações, treinamentos, melhores práticas, garantia e tecnologias que podem ser utilizadas para proteger a disponibilidade, integridade e confidencialidade de ativos nas infraestruturas conectadas pertencentes ao governo, organizações privadas e cidadãos” (ITU, 2018).

Sendo assim, a cibersegurança se configura como uma ferramenta cada vez mais necessária perante as incessantes ameaças virtuais.

Na intenção de evitar prejuízos e exposições, o mercado cada vez mais demanda a especialização de profissionais em cibersegurança dotados de conhecimentos técnicos em redes, servidores e ferramentas de segurança.

Fonte: Guia Completo para Entrada no Mundo da Cibersegurança, CECyber

Conhecimentos necessários - Soft Skills

Soft Skills são habilidades mais comportamentais, que se relacionam com as experiências vivenciadas pelo profissional ao longo dos anos.

Ainda que a área de cibersegurança seja repleta de tecnicidade, o desenvolvimento de soft skills não se dá através de certificações ou habilidades técnicas, e sua identificação é cada vez mais requisitada nos processos de seleção.

Fonte: Guia Completo para Entrada no Mundo da Cibersegurança, CECyber

Soft Skills

Comunicação

Uma comunicação eficaz é uma das ferramentas fundamentais para qualquer profissional que está inserido, ou pretende se inserir, no mercado de trabalho. Para o profissional de segurança cibernética, o domínio de uma boa comunicação é ainda essencial para que se possa transpor a linguagem técnica inerente à área aos demais setores de uma organização de forma inteligível.

Se dá através de certificações ou habilidades técnicas, e sua identificação é cada vez mais requisitada nos processos de seleção.

Fonte: Guia Completo para Entrada no Mundo da Cibersegurança, CECyber

Soft Skills

Colaboração

Aliada à comunicação eficaz, a boa relação com os demais setores da organização (como o setor financeiro, diretoria, recursos humanos, equipe de marketing e demais operações) é uma característica esperada dos especialistas em segurança cibernética.

Dispor de habilidades colaborativas e pessoais mais amplas facilita para que o trabalho tenha maior produtividade, e as metas e objetivos definidos alcançados com mais facilidade.

Fonte: Guia Completo para Entrada no Mundo da Cibersegurança, CECyber

Soft Skills

Resiliência

Em momentos de crise, a resiliência é possivelmente a soft skill mais necessária para o profissional de cibersegurança. Podemos classificar a resiliência como a capacidade de lidar e superar as adversidades. Por exemplo, quando ocorre um ataque cibernético em determinada empresa, é fundamental que o especialista consiga enfrentar as pressões impostas para dar andamento aos procedimentos necessários e conter as ameaças. Nesse sentido, é uma habilidade desenvolvida a partir da experiência e de boas capacitações.

Fonte: Guia Completo para Entrada no Mundo da Cibersegurança, CECyber

Soft Skills

Habilidades de pesquisa e redação

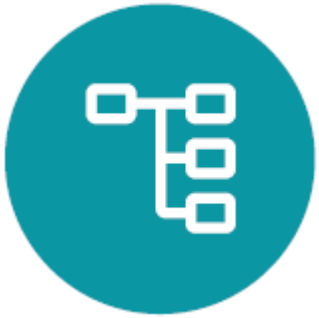
Os instintos de pesquisa e redação são ativos inestimáveis que qualquer analista de segurança da informação deve possuir. Tal habilidade ganha ainda mais destaque ao executar a criação e aplicação de políticas. Essencialmente, isso significa que a equipe de segurança cibernética deve conduzir pesquisas intensivas e trabalhar com os usuários finais para entender como a tecnologia é aproveitada diariamente.

Fonte: Guia Completo para Entrada no Mundo da Cibersegurança, CECyber

Soft Skills

Networking

As habilidades de networking dizem respeito à capacidade de manter e expandir os contatos profissionais e pessoais. Através do networking, é possível unificar grupos com interesses em comum para promover ações de alto valor. Logo, é uma habilidade fundamental no desenvolvimento da carreira do profissional de segurança cibernética.



Fonte: Guia Completo para Entrada no Mundo da Cibersegurança, CECyber

Soft Skills

Adaptabilidade

O profissional de cyber está em constante aprendizado. O cenário de ameaças de TI é constantemente alterado com novos vírus, worms e firewalls suscetíveis. Como especialista em segurança cibernética, você deve seguir e compreender as melhores práticas, métodos, padrões e tendências, bem como as fraquezas geradas pela Internet e estar preparado às constantes mudanças que envolvem a área.

Fonte: Guia Completo para Entrada no Mundo da Cibersegurança, CECyber

Conhecimentos necessários - Hard Skills

Diferentemente das soft skills, as hard skills são habilidades mais fáceis de quantificar. São competências aprendidas ao longo dos anos através de livros, trabalhos ou treinamentos, por exemplo. Logo, são habilidades mais voltadas à tecnicidade e frequentemente listadas em currículos e cartas de apresentação.

Fonte: Guia Completo para Entrada no Mundo da Cibersegurança, CECyber

Hard Skills

Conhecimento em configurações de servidores Windows e Linux

É esperado que o especialista tenha conhecimentos avançados com o sistema operacional Windows Server, como noções de instalação e configuração do Domain Controller, Active Directory e Gerenciamento de Políticas de Grupo – GPO, além de ser apto a realizar configuração de Serviços de Redes: DHCP, DNS, HTTP, HTTPS, FTP, File Server, Backup Server, entre outros.

Em relação ao sistema operacional Linux, espera-se conhecimentos em configuração de Serviços de Redes, como DHCP, DNS, HTTP, HTTPS, FTP, File Server, SSH Server e Samba-DC, em Interface de Linha de Comando (CLI) e Gerenciamento do Servidor Linux, além de Firewall Iptables e Análise de Logs.

Fonte: Guia Completo para Entrada no Mundo da Cibersegurança, CECyber

Hard Skills

Operação com Banco de Dados

É importante que o profissional saiba instalar e manipular banco de dados (como o Microsoft SQL Server, MySQL, Oracle, MongoDB e PostgreSQL), analisar logs e registros, construir e executar scripts automatizados, além de criar e restaurar backups físicos e lógicos.

Fonte: Guia Completo para Entrada no Mundo da Cibersegurança, CECyber

Hard Skills

Domínio em Redes de Computadores

Para se destacar na área, o profissional da área deve conhecer e compreender os fundamentos e protocolos de redes (TCP/IP, DHCP, DNS, ARP, HTTP, ICMP, entre outros). Projetar e analisar redes de computadores. Capturar e inspecionar pacotes e tráfegos de redes através de ferramentas como Wireshark e tcpdump. Monitorar ativos de redes (protocolos SNMP e RMON) via sistemas de gerenciamento de redes e ativos, como o Zabbix e o Zenoss Community.

Fonte: Guia Completo para Entrada no Mundo da Cibersegurança, CECyber

Hard Skills

Hardening de Estações e Servidores

Realizar operações de endurecimento (hardening) em banco de dados e sistemas operacionais (Windows e Linux) é outra hard skill exigida para quem quer atuar na área de cibersegurança.

Fonte: Guia Completo para Entrada no Mundo da Cibersegurança, CECyber

Hard Skills

Compreender linguagens de programação

Linguagens como Python, Shell Script, HTML, C, C++, Assembly, PHP e JavaScript são algumas das linguagens mais populares e desejáveis para os profissionais que pretendem atuar com a cibersegurança.

Fonte: Guia Completo para Entrada no Mundo da Cibersegurança, CECyber

Hard Skills

Capacidade para lidar com ferramentas de Segurança Cibernética

Ser apto a operar ferramentas de cibersegurança, como Firewall, IDS/IPS (Sistema de Detecção de Intrusão e Sistema de Prevenção de Intrusão), WAF (Web Application Firewall), Antivírus, DLP (Data Loss Prevention) e SIEM (Gerenciamento e Correlação de Eventos de Segurança) são fundamentais para que quer seguir uma carreira de sucesso na área.

Fonte: Guia Completo para Entrada no Mundo da Cibersegurança, CECyber

Times de cibersegurança

Red team ou “time vermelho” diz respeito aos grupos especializados na penetração de sistemas. Dessa forma, essa equipe busca testar a eficácia de um programa de segurança, simulando ataques de forma realista a fim de extrair relatórios e expor possíveis vulnerabilidades.

Em outras palavras, são dedicados ao “Offensive Security”, ou seja, à invasão de sistemas para que melhorias e aprimoramentos possam ser desenvolvidos.

Fonte: Guia Completo para Entrada no Mundo da Cibersegurança, CECyber

Times de cibersegurança

Blue team ou “time azul” são as equipes dedicadas à defesa de qualquer tipo de ameaça de uma organização. Por isso, realizam coleta de dados, análises dos dados, sistemas, redes e servidores que devem ser protegidos, além de produzirem avaliações de riscos, ou seja, as possíveis vulnerabilidades suscetíveis às ameaças cibernéticas. A partir de tais ações, os profissionais dessa categoria desenvolvem e implementam políticas e planos de ações para reduzir as probabilidades de um eventual ataque.

Fonte: Guia Completo para Entrada no Mundo da Cibersegurança, CECyber

Times de cibersegurança

Purple team ou “time roxo”, por sua vez, são aquelas que garantem que as equipes vermelhas e azuis se mantenham em constante comunicação e colaboração. Logo, é o time que capta as estratégias e planos defensivos do Time Azul, e unifica com as informações sobre as ameaças e vulnerabilidades encontradas pelo Time Vermelho. Assim, os resultados obtidos de ambas as equipes são maximizados, e a segurança da organização obtém melhorias significativas. O Time Roxo garante que as perspectivas defensiva e ofensiva estejam em constante comunicação. O purple team pode ser organizado como uma equipe própria, assim como o red e o blue, ou como uma dinâmica contínua das demais.

Fonte: Guia Completo para Entrada no Mundo da Cibersegurança, CECyber

Times de cibersegurança

Os membros do yellow team seriam aqueles responsáveis por projetarem softwares e sistemas de uma empresa ou organização, considerando-se a abordagem do desenvolvimento seguro de software. Logo, engenheiros de software e desenvolvedores de aplicativos, por exemplo, poderiam ser enquadrados como parte de um Time Amarelo.

Fonte: Guia Completo para Entrada no Mundo da Cibersegurança, CECyber

Times de cibersegurança

O orange team ou “time laranja” seria a junção do yellow team com os conhecimentos do red team. Em outras palavras, é treinar o desenvolvedor com a mentalidade de um invasor, para que sejam formados melhores programadores, e os sistemas e aplicações desenvolvidos com protocolos de segurança mais robustos.

Fonte: Guia Completo para Entrada no Mundo da Cibersegurança, CECyber

Times de cibersegurança

Por fim, o green team (“time verde”) une os conhecimentos do blue team com as atuações do yellow team. Com o feedback do Time Azul, é possível, nos momentos iniciais do desenvolvimento de uma aplicação ou sistema, identificar vulnerabilidades e elaborar estratégias que tornem o ativo mais seguro.

Fonte: Guia Completo para Entrada no Mundo da Cibersegurança, CECyber

Certificações

Cisco Certified Network Associate (CCNA) Routing and Switching

A certificação CCNA Routing and Switching da fabricante Cisco é considerada como uma das bases para a área de redes. Ela possui a finalidade de validar a capacidade de instalar, configurar, operar e solucionar problemas de redes de Roteadores e Switches de tamanho médio. Possui validade de 03 (três) anos.

Fonte: Guia Completo para Entrada no Mundo da Cibersegurança, CECyber

Certificações

CompTIA Network+

Também relacionada a redes e com validade de 03 (três) anos, a certificação Network+ da CompTIA assegura que o profissional é capacitado para: projetar e implementar redes funcionais; configurar, gerenciar e manter dispositivos de redes essenciais; utilizar dispositivos como switches e roteadores para segmentar o tráfego de rede e criar redes resilientes; identificar benefícios e desvantagens das configurações de rede existentes; implementar segurança de rede, padrões e protocolos; solucionar problemas de rede e dar suporte na criação de redes virtualizadas.

Fonte: Guia Completo para Entrada no Mundo da Cibersegurança, CECyber

Certificações

CompTIA Security+

Considerada como uma das certificações básicas para a Segurança da Informação. O exame exigirá que o profissional consiga avaliar a postura de segurança de um ambiente corporativo e recomendar e implementar soluções de segurança apropriadas; monitorar e proteja ambientes híbridos, incluindo nuvem, celular e IoT; operar com consciência das leis e políticas aplicáveis, incluindo princípios de governança, risco e conformidade; identificar, analisar e responder a incidentes e eventos de segurança. Assim como as anteriores, possui validade durante 03 (três) anos.

Fonte: Guia Completo para Entrada no Mundo da Cibersegurança, CECyber

Certificações

Certified Ethical Hacker (CEH)

Exame da EC-Council centrado no teste de conhecimentos como ameaças à segurança da informação e vetores de ataque, detecção de ataques, prevenção de ataques, procedimentos e metodologias.

Fonte: Guia Completo para Entrada no Mundo da Cibersegurança, CECyber

Certificações

CompTIA PenTest+

Exame responsável por avaliar todas as fases de penetração e gerenciamento de vulnerabilidades. A obtenção do certificado assegura que o profissional é capaz de planejar e definir o escopo de um compromisso de teste de penetração; entender os requisitos legais e de conformidade; executar a verificação de vulnerabilidade e teste de penetração usando ferramentas apropriadas e técnicas e, em seguida, analisar os resultados; produzir um relatório escrito contendo técnicas de remediação propostas, e de forma eficaz comunicar os resultados à equipe de gestão, fornecendo recomendações práticas.

Fonte: Guia Completo para Entrada no Mundo da Cibersegurança, CECyber

Certificações

Offensive Security Certified Professional (OSCP)

Trata-se de uma certificação direcionada àqueles que buscam carreira no Hacking Ético ou pen testing. Desenvolvida pela Offensive Security, o exame avaliará as habilidades do candidato em utilizar várias ferramentas para pentesting dentro do sistema operacional Kali Linux, ao mesmo tempo em que documentam quaisquer vulnerabilidades nos exercícios de laboratório. Os examinadores não estarão apenas preocupados com as habilidades técnicas, mas também com a comunicação profissional e as habilidades de documentação adequadas, que são um requisito para a maioria das funções de TI.

Fonte: Guia Completo para Entrada no Mundo da Cibersegurança, CECyber

Certificações

CompTIA CySA+

A certificação CySA+ da CompTIA aplica análises comportamentais a redes e dispositivos para prevenir, detectar e combater ameaças de segurança cibernética por meio de monitoramento contínuo da segurança. O candidato que busca tal certificação terá que demonstrar conseguir aproveitar as técnicas de inteligência e detecção de ameaças; analisar e interpretar dados; identificar e resolver vulnerabilidades; sugerir medidas preventivas e responder e se recuperar efetivamente de incidentes.

Fonte: Guia Completo para Entrada no Mundo da Cibersegurança, CECyber

Certificações

Certified Incident Handler (ECIH)

Emitido pela EC-Council, a certificação ECIH é um programa abrangente de nível especialista que transmite conhecimentos e habilidades que as organizações precisam para lidar efetivamente com as consequências pós-violação, reduzindo o impacto do incidente, tanto do ponto de vista financeiro quanto de reputação.

Fonte: Guia Completo para Entrada no Mundo da Cibersegurança, CECyber

Para saber mais...

… leia o Guia Completo para Entrada no Mundo da Cibersegurança, da CECyber.

Módulo 13

Oportunidades de pesquisa em Segurança da Informação

Pesquisa acadêmica

Uma pesquisa é um trabalho de investigação que um indivíduo realiza com a intenção de descobrir algo. Enquanto a pesquisa científica tem como foco o desenvolvimento de uma tecnologia ou descoberta dentro das ciências, a acadêmica pretende que o realizador aprenda algo sobre o assunto pesquisado. É por isso que o nome dado é pesquisa acadêmica: a intenção é que a pessoa se aprofunde na academia, sejam professores ou alunos.

A pesquisa acadêmica é um exercício de estudo e aprendizado em primeiro lugar, mas não deixa de ser um esforço para acrescentar algo ao mundo. É a partir desse estudo que as ideias científicas podem surgir.

Fonte: Pesquisa Acadêmica, por Gildenir Carolino Santos, in Blog do Portal de Periódicos Eletrônicos Científicos, UNICAMP

Pesquisa acadêmica

O passo a passo para fazer uma pesquisa acadêmica é o seguinte:

- Escolha do tema
- Metodologia
- Consulta às fontes
- Normas
- Redação
- Revisão

Fonte: Pesquisa Acadêmica, por Gildenir Carolino Santos, in Blog do Portal de Periódicos Eletrônicos Científicos, UNICAMP

Pesquisa acadêmica

Escolha do tema:

Quando o trabalho está sendo realizado como uma parcela do aprendizado dentro de um curso, o tema geralmente é escolhido pelo professor.

Quanto o trabalho é destinado a um congresso, parte de uma iniciação científica ou um Trabalho de Conclusão de Curso (TCC), a escolha do tema é do autor.

Fonte: Pesquisa Acadêmica, por Gildenir Carolino Santos, in Blog do Portal de Periódicos Eletrônicos Científicos, UNICAMP

Pesquisa acadêmica

Metodologia:

A metodologia tem por função facilitar a comprovação das conclusões da pesquisa, pois ela permite que tudo seja feito de forma organizada e planejada, e garante que ela possa ser reproduzida.

As metodologias variam, mas em geral, para as pesquisas acadêmicas, o método mais comum é o da pesquisa bibliográfica.

Fonte: Pesquisa Acadêmica, por Gildenir Carolino Santos, in Blog do Portal de Periódicos Eletrônicos Científicos, UNICAMP

Pesquisa acadêmica

Consulta às fontes:

Para qualquer pesquisa, em especial a acadêmica, é muito importante contar com fontes de informações confiáveis e respeitadas.

Além dos livros, entre as fontes de pesquisa confiáveis estão o Portal de Periódicos da CAPES e o Google Scholar.

Fonte: Pesquisa Acadêmica, por Gildenir Carolino Santos, in Blog do Portal de Periódicos Eletrônicos Científicos, UNICAMP

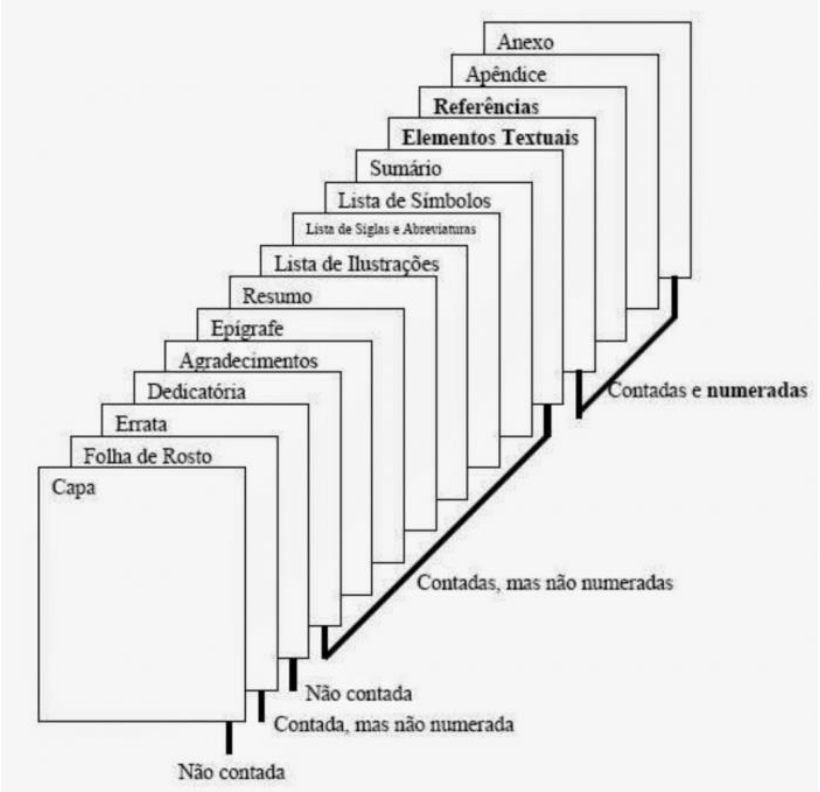
Pesquisa acadêmica

Normas:

As normas técnicas auxiliam na formatação do texto e elas são parte do que dá clareza e entendimento ao trabalho acadêmico.

Algumas das normas brasileiras utilizadas são as seguintes:

- ABNT NBR 14724: Informação e documentação – Trabalhos acadêmicos – Apresentação;
- ABNT NBR 10520: Informação e documentação – Citações em documentos – Apresentação;
- Entre outros.



Fonte: Pesquisa Acadêmica, por Gildenir Carolino Santos, in Blog do Portal de Periódicos Eletrônicos Científicos, UNICAMP

Pesquisa acadêmica

Redação:

Um trabalho acadêmico é composto de elementos pré-textuais, textuais e pós-textuais.

- Elementos pré-textuais: Capa, Folha de Rosto, Resumo e Sumário;
- Elementos textuais: Introdução, Desenvolvimento e Conclusão;
- Elementos pós-textuais: Referência Bibliográfica e eventuais anexos.

Fonte: Pesquisa Acadêmica, por Gildenir Carolino Santos, in Blog do Portal de Periódicos Eletrônicos Científicos, UNICAMP

Pesquisa acadêmica

Redação – elementos textuais:

A Introdução é onde será contextualizado o trabalho, explicando a importância e relevância do mesmo e justificando a decisão da escolha temática e metodológica.

O Desenvolvimento é onde o método é aplicado ao tema escolhido com apoio das fontes apresentadas e os dados relevantes são apresentados.

A Conclusão é onde os dados apresentados no Desenvolvimento serão analisados e se tentará apresentar uma resposta partindo deles. Esse elemento textual não precisa ser categórico em suas afirmações, apenas realista com relação aos resultados obtidos.

Fonte: Pesquisa Acadêmica, por Gildenir Carolino Santos, in Blog do Portal de Periódicos Eletrônicos Científicos, UNICAMP

Pesquisa acadêmica

Revisão:

Uma vez com o trabalho escrito, é de suma importância realizar uma revisão para garantir que o trabalho está correto e tudo está dentro do esperado.

É interessante pedir que pessoas de fora da pesquisa leiam o texto final para procurarem incongruências na sua argumentação, bem como fazer uma verificação da ortografia e procurar por erros gramaticais.

Por fim, é de suma importância que se verifiquem as normas técnicas, em especial as da Associação Brasileira de Normas Técnicas (ABNT), de forma que a pesquisa acadêmica esteja dentro das regras esperadas.

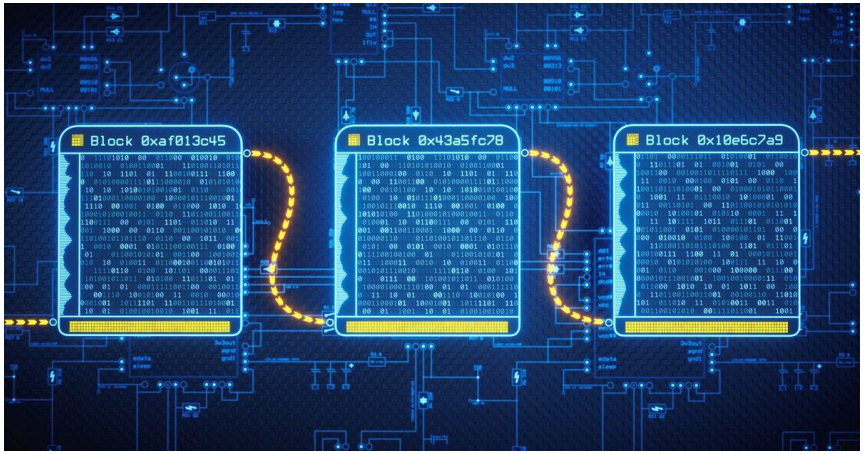
E o mais importante: NUNCA PRATIQUE PLÁGIO!

Fonte: Pesquisa Acadêmica, por Gildenir Carolino Santos, in Blog do Portal de Periódicos Eletrônicos Científicos, UNICAMP

Pesquisa acadêmica
Temas em Segurança da Informação

Blockchain:

A blockchain é uma espécie de livro-razão compartilhado e imutável usado para registrar transações, rastrear ativos e aumentar a confiança.



A blockchain pode ser utilizada em segurança da informação para garantir a rastreabilidade e impedir fraudes.

Fonte: ibm.com

Pesquisa acadêmica
Temas em Segurança da Informação

Computação em nuvem:

A computação em nuvem permite terceirizar as operações de datacenter a um custo mais baixo e ampliar as capacidades de processamento de forma elástica.

Este novo paradigma amplia a superfície de ataque e o perímetro de segurança a ser protegido, de forma que novas técnicas devem ser adotados para proteger a nuvem híbrida (combinação de nuvens pública e privada.)

Pesquisa acadêmica
Temas em Segurança da Informação

Internet da Coisas:

A Internet das Coisas diz respeito a todos os objetos com sensores e/ou atuadores que estão conectados na rede mundial de computadores, a Internet.

A Internet das Coisas aumenta a complexidade dos processos de segurança da informação pois nem sempre é possível garantir a segurança física dos dispositivos.

Pesquisa acadêmica
Temas em Segurança da Informação

Traga Seu Próprio Dispositivo (Bring Your Own Device):

O BYOD é um conceito de infraestrutura que consiste na utilização dos aparelhos dos próprios funcionários para desempenhar as atividades empresariais.

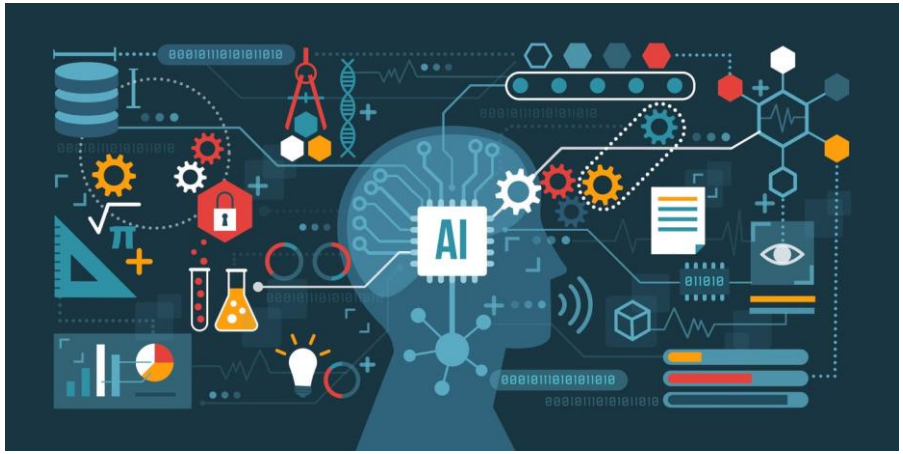
Com o BYOD, é necessário reformular as políticas de uso e estratégias de segurança, bem como investir na conscientização dos usuários para o correto uso e a implementação de ferramentas para atualização de segurança dos dispositivos.

Fonte: softwareone.com

Pesquisa acadêmica
Temas em Segurança da Informação

Inteligência artificial:

A inteligência artificial refere-se a sistemas ou máquinas que imitam a inteligência humana para executar tarefas e podem se aprimorar iterativamente com base nas informações que coletam.



A inteligência artificial pode ser utilizada para detectar e impedir intrusões de segurança, uma vez que ela utiliza análise de comportamento para identificar os diferentes tipos de ameaças.

Fonte: oracle.com

Para saber mais...

… leia a matéria **Pesquisa Acadêmica: Tudo o que você precisa saber**, de Gildenir Carolino Santos, disponível em https://periodicos.sbu.unicamp.br/blog/index.php/2018/09/15/pesquisa-academica/

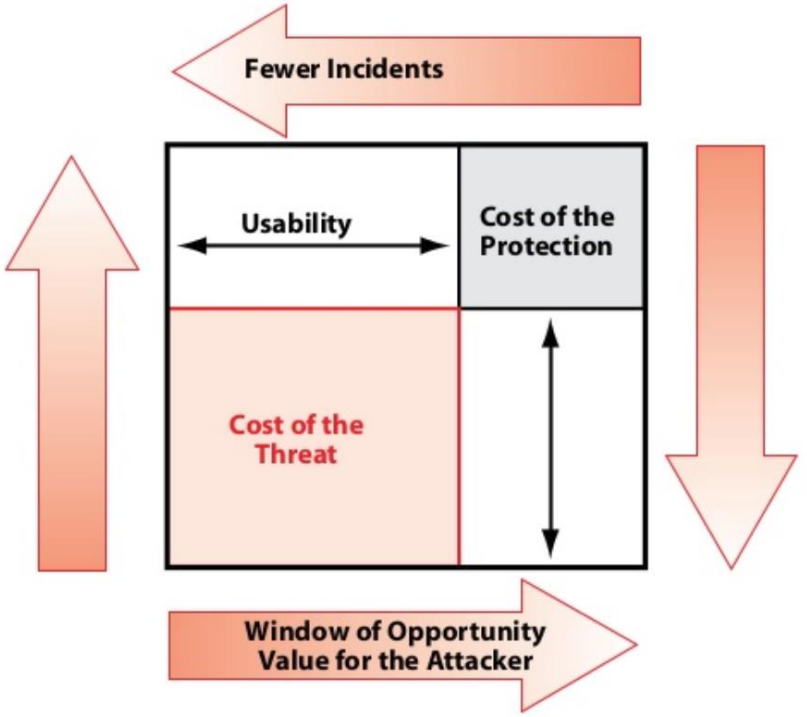
Módulo 14

Return on Security Investment

Introdução

O Retorno do Investimento de Segurança, também conhecido como ROSI (Return On Security Investment), é um método para calcular e determinar se um conjunto de medidas de segurança que tem por objetivo mitigar ou reduzir os riscos de segurança vale ou não a pena ser implementado.

Em outras palavras, para que um conjunto de medidas de segurança seja financeiramente viável, a redução do risco deve ser maior do que o custo de implementação destas medidas.



Return on Investiment

No mundo das finanças e dos negócios, o investimento de capital deve ser medido pela sua eficácia em gerar rentabilidade para a organização. É aí que entra o cálculo do Retorno do Investimento, ou ROI (Return on Investiment), para a avaliação de um investimento.

O ROI é um índice de rentabilidade para um investimento específico. Ele ajuda a determinar se devemos fazer o investimento ou simplesmente ignorá-lo.

Para que um investimento seja justificado, deve expressar em termos quantitativos por que precisa acontecer. As propostas com o maior potencial de rentabilidade geralmente vencem, e é por isso que as propostas de segurança da informação muitas vezes perdem. O cálculo típico do retorno do investimento é dado por:

$$ROI = \frac{Ganho\ do\ Investimento - Custo\ do\ Investimento}{Custo\ do\ Investimento}$$

Fonte: How to calculate your return on security investments, Isaac Kohen

ROI vs ROSI

Por que o ROI clássico não funciona para retorno do investimento em segurança?

A equação do ROI funciona apenas para investimentos que geram resultados positivos, como redução de custos ou aumento de receita.

Mas o que é um investimento em segurança?

Um investimento em segurança não aumenta as receitas diretamente e nem fornece retorno imediato. Em vez disso, os investimentos em segurança dizem respeito ao gerenciamento de riscos que resultam em prevenção de perdas e mitigação de riscos. Em outras palavras, a segurança em geral não é um investimento que fornece lucro, mas que previne as perdas.

Assim, um cálculo do ROSI deve indicar quanta perda a organização poderia evitar devido ao investimento em segurança, por isso se faz necessária uma fórmula diferente.

Fonte: How to Calculate Return on Security Investment, Matt Middleton-Leal

Conceitos de avaliação de risco

Para quantificar o impacto da segurança da informação nos negócios, o risco precisa ser determinado. Os seguintes conceitos de risco serão a base do cálculo do ROSI.

Expectativa de Perda Única ou SLE (Single Loss Expectancy)

O SLE é a quantia esperada de dinheiro que será perdida quando ocorrer um risco. Nesta abordagem, o SLE pode ser considerado como o custo total de um incidente, assumindo sua única ocorrência.

Devido à natureza específica do incidente de segurança, a maior complexidade é levar em conta todos os ativos em que esse incidente tem impacto. Por exemplo, um laptop roubado não apenas custará a substituição do laptop em si, mas também implicará em perda de produtividade, perda de reputação, tempo de suporte de TI e, possivelmente, custo de perda de propriedade intelectual.

Fonte: Introduction to Return on Security Investment, da European Network and Information Security Agency

Conceitos de avaliação de risco

Taxa Anual de Ocorrência ou ARO (Annual Rate of Occurrence)

A ARO é uma medida da probabilidade de um risco ocorrer em um ano.

Estes dados são uma aproximação e podem depender de muitos fatores. Por exemplo, a ARO de uma inundação dependerá de fatores geográficos, a ARO de uma falha de disco é influenciado pela temperatura de operação, a ARO de um arrombamento dependerá da localização do ativo, e claro, a ARO também depende das medidas de segurança existentes. A ARO de um ataque de código malicioso bem-sucedido diminuirá significativamente após a implementação de um antivírus eficaz.

Uma forma de medir a ARO é avaliando o histórico de ocorrências.

Fonte: Introduction to Return on Security Investment, da European Network and Information Security Agency

Conceitos de avaliação de risco

Expectativa Anual de Perdas ou ALE (Annual Loss Expectancy)

A ALE é a perda monetária anual que pode ser esperada de um risco específico sobre um ativo específico.

A ALE é dada por:

$$ALE = ARO \times SLE$$

Fonte: Introduction to Return on Security Investment, da European Network and Information Security Agency

Conceitos de avaliação de risco

Expectativa Anual de Perda Modificada ou mALE (Modified Annual Loss Expectancy)

A implementação de uma solução de segurança eficaz reduz a ALE. Quanto mais eficaz é uma solução, mais reduzida a ALE será. Essa redução da perda monetária pode ser definida pela diferença entre a ALE sem a solução de segurança e a ALE modificada (mALE) que implementa a solução de segurança.

$$mALE = ALE \times (1 - Taxa\ de\ Mitigação)$$

Fonte: Introduction to Return on Security Investment, da European Network and Information Security Agency

Cálculo do ROSI

O cálculo do ROSI combina a avaliação quantitativa de riscos e o custo da implementação de medidas de segurança para esse risco. No final, compara a ALE com a perda esperada. A fórmula do ROSI é dada por:

$$ROSI = \frac{ALE - mALE - Custo\ da\ Solução}{Custo\ da\ Solução}$$

-- ou --

$$ROSI = \frac{ALE \times Taxa\ de\ Mitigação - Custo\ da\ Solução}{Custo\ da\ Solução}$$

-- ou --

$$ROSI = \frac{(ARO \times SLE) \times Taxa\ de\ Mitigação - Custo\ da\ Solução}{Custo\ da\ Solução}$$

Fonte: Introduction to Return on Security Investment, da European Network and Information Security Agency

Cálculo do ROSI – Exemplo

A empresa ACME está pensando em investir em uma solução antivírus. A cada ano a empresa sofre 5 ataques de vírus (ARO = 5). O CSO (Chief Security Officer) estima que cada ataque custa aproximadamente US$ 15.000 em perda de dados e produtividade (SLE = 15.000). Espera-se que a solução antivírus bloqueie 80% dos ataques (Taxa de Mitigação = 80%) e ela custará US$ 25.000 por ano (incluindo taxas de licença, treinamento, instalação, manutenção, etc.).

O retorno do investimento em segurança para essa solução será dado por:

$$ROSI = \frac{(ARO \times SLE) \times Taxa\ de\ Mitigação - Custo\ da\ Solução}{Custo\ da\ Solução}$$

$$ROSI = \frac{(5 \times 15000) \times 80\% - 25000}{25000} = \boxed{140\%}$$

Fonte: Introduction to Return on Security Investment, da European Network and Information Security Agency

Para saber mais...

… leia o documento Introduction to Return on Security Investment, da European Network and Information Security Agency

FIM