SEGURANÇA INFORMÁTICA E DAS COMUNICAÇÕES

- Ficha de Apoio -

CAPÍTULO 1. FUNDAMENTOS DE SEGURANÇA DA INFORMAÇÃO

1. Introdução à Segurança da Informação

Segurança da informação é o conjunto de políticas, acções, métodos e ferramentas destinadas a proteger os bens informáticos de uma Organização.

O sistema de informação define-se geralmente como o conjunto dos dados e dos recursos materiais e *softwares* da organização que permite armazená-los ou fazê-los circular. O sistema de informação representa um património essencial da organização, que deve ser protegido. De um modo geral, a segurança informática consiste em garantir que os recursos materiais ou *softwares* de uma organização sejam utilizados apenas no âmbito previsto.

A ameaça representa o tipo de acção susceptível de prejudicar a organização, enquanto a vulnerabilidade (às vezes chamada de falha ou brecha) representa o nível de exposição à ameaça em um contexto específico. A medida defensiva é o conjunto das acções implementadas para a prevenção da ameaça. As medidas defensivas a serem aplicadas não são apenas soluções técnicas, mas também medidas de

formação e sensibilização para os usuários, assim como um conjunto de regras claramente definidas.

A fim de poder proteger um sistema, é preciso identificar as ameaças potenciais e, consequentemente, conhecer e prever a maneira de prevenir do inimigo, tendo atenção as seguintes questões:

a) O que pretendemos proteger?
b) Porque pretendemos proteger?
c) De quem pretendemos proteger?
d) Como devemos proteger?

2. Condições para a Segurança da Informação

A segurança de uma organização deve ser analisada num contexto alargado, tomando-se em consideração todas as diferentes perspectivas como, por exemplo, dados, operações, aplicações e acesso físico, entre muitas outras.

A crescente utilização da tecnologia da informação em todos âmbitos da actividade económica, pública ou privada, demostra ser merecedora de confiança.

Basta a experiência comum para perceber a dependência das organizações (e da sociedade) de uma tecnologia que se desenvolve a cinco décadas a um ritmo desconhecido na história das invenções. Por sua vez, essa tecnologia tem exercido sua influência na inovação dos campos do saber onde tem sido aplicada.

A dependência em relação a tecnologia da informação, e a necessidade de um desenvolvimento sustentável da Sociedade da Informação ou Sociedade em Rede reclama o estabelecimento dos fundamentos sólidos dessa confiança. O que significa aplicar salvaguardas ou defesas (técnicas e administrativas) visando controlar o risco e o dispor de legislação que sirva para marcar as regras do jogo, dirimir as discrepâncias e castigar o delito em relação as violações.

A segurança deve ser feita de forma integrada e abrangente, no entanto, assiste-se com frequência à limitação desta abrangência, por parte dos responsáveis de segurança da organização, que se restringem às questões associadas à segurança física, sendo a área da informática, quando existe, tratar das restantes medidas de segurança, sem ter como base uma política que reflita toda a organização. Não existindo um plano único, integrado, de segurança, transmite a ideia que a informática da organização não seja tão

importante ou não contivesse a informação essencial para o negócio, como o edifício onde a mesma tem sede. O paradoxo desta situação é que a inexistência de um plano integrado de segurança pode levar, por si só, a existência de potenciais lacunas graves. Para quê colocar grades nas janelas de uma casa cuja porta das traseiras é de vidro comum ou de estacas e não tem qualquer outra protecção? O mesmo acontece com a integração da segurança empresarial como um todo. Apesar da maior tendência ser garantir a segurança na comunicação de dados, este é apenas um dos elos da cadeia de segurança, podendo ser comprometida pela fraca segurança de outro elo qualquer. Não serve de nada ter um sistema sofisticado de cifra, se um estranho lhe pode aceder fisicamente e desligá-lo!

O processo de segurança não é algo meramente executado por um pequeno grupo de pessoas no seio da organização, porém, envolve todas as pessoas da organização. Começar pelo topo e fazer reflectir essa sensibilização para baixo, na estrutura organizacional, pode ser a diferença entre o sucesso e o insucesso de todo o processo.

A segurança na organização deve então constituir-se como um processo, cuja execução capacita na protecção da sua infra-estrutura e no controlo de acesso à sua informação. A segurança não deve, nesta perspectiva, ser entendida como um conjunto de elementos tecnológicos de ponta, mas antes como algo que é aplicado de forma horizontal e consistente na organização, sendo regularmente monitorada e avaliada. Na figura abaixo, ilustram-se os passos os passos a seguir para a definição e implementação do processo de segurança da organização.

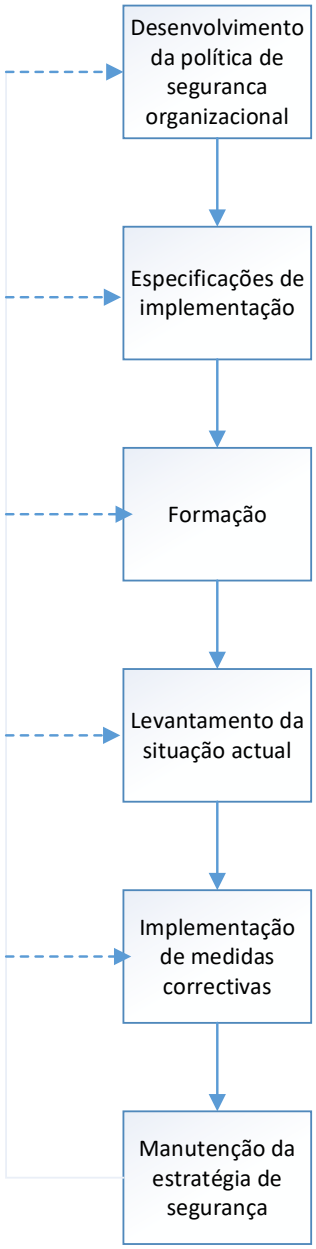


Figura – Passos para a criação do processo de segurança na organização

O desenvolvimento de uma política de segurança organizacional compreensível deverá ser primeiro passo na melhoria da segurança global de qualquer organização, pois será a partir desta que serão desenvolvidos os *standards* de segurança aos níveis inferiores, como por exemplo, para a rede informática e para os computadores. Estes *standards* traduzem na prática, a política de segurança nos mecanismos necessários para à sua realização, os *standards* servem também para definir as especificações de implementação que

vem contidos num documento que serve de orientação aos administradores de sistemas para a implementação da política de segurança.

A politica de segurança deve vir expresso em um documento aprovado pela gestão sénior da organização que terá que ser seguida ao pé da letra do que esta estabelecido. As políticas de segurança devem ter implementação realista, e definir claramente as áreas de responsabilidade dos utilizadores, do pessoal de gestão de sistemas e redes e da direcção. Deve também adaptar-se a alterações na organização. As políticas de segurança fornecem um enquadramento para a implementação de mecanismos de segurança, definem procedimentos de segurança adequados, processos de auditoria à segurança e estabelecem uma base para procedimentos legais na sequência de ataques. Devem ser efectuadas auditorias constantes a Politica de Segurança, estas auditorias fornecem uma imagem temporal da situação no momento, mas não constituem nenhuma forma de protecção contra alterações a configurações.

Deve haver um processo contínuo no tempo, com diferentes facetas, como por exemplo: a recepção, análise e distribuição de alertas de segurança, ou a implementação de mecanismos que assegurem que qualquer alteração com impacto na segurança de qualquer sistema despoleta uma reavaliação do plano se segurança.

3. Normas de Segurança

As normas de segurança da informação desempenham um papel fundamental na protecção dos sistemas e dos dados sensíveis em um ambiente digital cada vez mais complexo e ameaçador.

A família ISO 27000 é uma série de normas internacionais que se concentra na gestão da segurança da informação. Essas normas são desenvolvidas pela Organização Internacional de Normalização (ISO) e pela Comissão Electrotécnica Internacional (IEC) e são projectadas para ajudar as organizações a estabelecerem, implementarem e manterem sistemas de gestão de segurança da informação eficazes (A. P. Monteiro e Chagas 2023).

Segundo (A. P. Monteiro e Chagas 2023), as Normas de Segurança da Informação família ISO 27000 são:

- **ISO/IEC 27001:** estabelece os requisitos para um Sistema de Gestão de Segurança da Informação (SGSI) e sua certificação;

- **ISO/IEC 27002:** directrizes e requisitos para a segurança da informação em organizações, incluindo um conjunto de controles e boas práticas;
- **ISO/IEC 27003:** orientações para a implementação de um sistema de gestão de segurança da informação em uma organização;
- **ISO/IEC 27004:** norma para medir e avaliar a segurança da informação;
- **ISO/IEC 27005:** norma que trata de gerenciamento de riscos de segurança da informação;
- **ISO/IEC 27007:** norma que fornece directrizes para auditorias internas de sistemas de gestão de segurança da informação;
- **ISO/IEC 27014:** norma que fornece directrizes para governança de segurança da informação;
- **ISO/IEC 27031:** norma que aborda a continuidade de negócios e a gestão de segurança da informação;
- **ISO/IEC 27032:** trata da segurança cibernética, fornecendo directrizes e princípios gerais para proteger sistemas, redes e informações contra ameaças cibernéticas;
- **ISO/IEC 27037:** trata de directrizes e princípios para identificar, colectar e preservar evidências digitais em investigações de segurança da informação; e
- **ISO/IEC 27701:** norma sobre privacidade da informação.

Essas normas estabelecem directrizes e práticas recomendadas para garantir a confidencialidade, integridade e disponibilidade da informação, bem como a gestão adequada dos riscos associados.

4. Principios básicos de Segurança da Informação

A segurança da informação é um dos temas mais importantes dentro das organizações em função do grande número de ataques virtuais orquestrados por cibercriminosos no mundo todo. Devido a isso, esse tópico se tornou um objectivo constante não só das equipes de TI, como das próprias organizações. Contudo, para que ele possa ser reforçado nas empresas, é preciso atenção aos três pilares que sustentam a segurança em TI: Confidencialidade, Integridade e Disponibilidade.

Cada um desses itens tem vital importância para os processos de proteção de dados, sendo essenciais em qualquer política interna de Tecnologia da Informação voltada a garantir que os processos internos fluam corretamente.

Confidencialidade (*Confidentiality*)

Modo de garantir que a informação estará acessível apenas para pessoas autorizadas. A principal forma de mantê-la é por meio da autenticação, controlando e restringindo os acessos. Ela impõe limitações aos milhares de dados sigilosos que as empresas possuem. Sem a confidencialidade, as organizações ficam vulneráveis a ciber-ataques, roubo de informações confidenciais e até utilização de dados pessoais de clientes, o que pode causar diversos prejuízos, inclusive financeiros, este faz o uso dos recursos de Certificado Digital, Criptografia, Biometria e Senhas.

Se por exemplo, se uma base de dados não tiver restrição de acesso a usuários (acesso somente de pessoas cadastradas), então os dados cadastrados podem esvaziar (acedidos indevidamente), gerando uma quebra de confidencialidade.

Figura: O conteúdo da mensagem não pode ser entendido pelo atacante

Integridade (*Integrity*)

Princípio de integridade refere-se à manutenção das condições iniciais das informações de acordo com a forma que foram produzidas e armazenadas. Ou seja, a informação mantém sua origem e ela não pode ser

alterada, assim somente pessoas autorizadas poderão aceder e modificar os dados do sistema. Quando o processo é executado estrategicamente é possível utilizar ferramentas para realizar a recuperação de informações danificadas ou perdidas. Manter informação buscando preservá-la contra modificações ou destruição imprópria incluindo a irretratabilidade (não-repudio) [1] e autenticidade [2]. Suponha que um servidor seja invadido e dados tenham sido alterados sem que se tenha mecanismos de *backup*, nesse caso o princípio da integridade das informações foi comprometido.

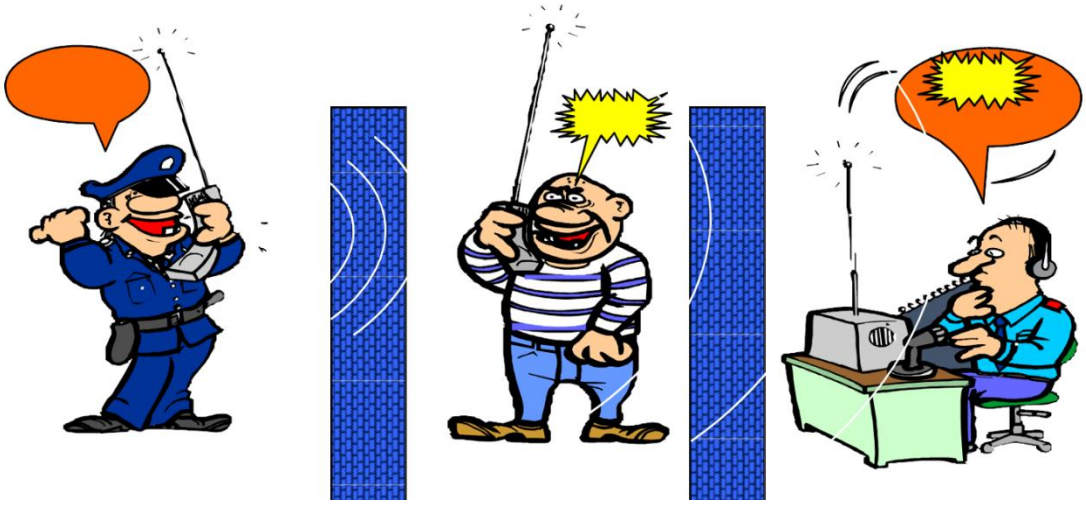


Figura: Qualquer alteração da mensagem por um atacante é detetável

Disponibilidade (*Availability*)

Dados corporativos precisam estar seguros e disponíveis para serem acedidos a qualquer momento pelos usuários autorizados. Esse princípio diz respeito à eficácia do sistema e do funcionamento da rede para que seja possível utilizar a informação quando necessário. Ela deve ser hospeda em um sistema à prova de falhas lógicas e redundantes. É essencial montar um Plano de Recuperação de Desastres (PRD) que contenha procedimentos e diretrizes para se administrar crises, manter a continuidade dos negócios e recuperar dados perdidos.

[1] *Não-repudio* consiste em provar que um indivíduo realizou uma determinada acção e num determinado momento.
[2] *Autenticidade* é a qualidade ou estado de ser genuíno ou original, ao invés de uma reprodução ou fabricação.

5. Recursos de Segurança

Os recursos de segurança são vários, no entanto, eles são aplicados em função das necessidades, podemos destacar os seguintes: *Hash*, Assinatura Digital, Criptografia, *Firewall*, *Proxy*, *Backup*, DMZ, RAID, Portas, Senhas, Biometria, IDS, IPS, *Bastion Host*, *No break*, entre outros.

6. Senhas *(Passwords)*

"Assume your adversary is capable of one trillion guesses per second." - **Edward Snowden**[3]

Senhas são de certo modo difíceis de memorizar, porém necessárias. Nos meios electrónicos, ainda não existe recurso de segurança que consiga ser mais viável do que elas. Bancos, cartões de crédito, contas de e-mail, redes sociais e lojas *on-line* estão entre as numerosas aplicações que dependem dessas combinações. A senha não pode ser óbvia. Caso ela seja, certamente que será fácil para muita gente descobrir e conseguirá acede-la. Esse tipo de código não sofre tanto com ataques de robôs programados para testar milhares de senhas por minuto, mas pode ser quebrado por pessoas mal-intencionadas que já conhecem as vítimas.

COMO NÃO CRIAR SENHAS

Não criar senhas baseadas em sequências

Senhas sequenciais são fáceis de decorar, por outro lado, podem ser descobertas com poucas tentativas. Combinações como **123456**, **abcdef**, **1020304050** ou **qwerty** (sequência do teclado).

Não usar dados e datas pessoais

Não usar data de aniversário de um parente, data de casamento, número da matrícula do carro, o número da residência, o número do telefone, o nome do filho, o sobrenome invertido, entre outros.

[3] https://theintercept.com/2015/03/26/passphrases-can-memorize-attackers-cant-guess/

Não utilizar palavras que estão ao redor para criar senhas

A marca do relógio na parede do escritório, o modelo do monitor de vídeo na sua mesa, o nome da loja que se vê quando se olha pela janela, especialmente quando se trata de um termo longo e difícil de ser assimilado na primeira tentativa.

Não criar senhas parecidas com as anteriores

Muitos sistemas exigem ou recomendam a troca periódica de senhas.

COMO ELABORAR UMA BOA SENHA

Misturar letras, símbolos especiais e números

Deve-se criar senhas misturando letras, símbolos especiais e números, pode-se utilizar uma palavra como base, mas substituir alguns de seus caracteres. Por exemplo, em vez de escrever **ISUTC** como senha, escreva **!5u7c**.

Usar letras maiúsculas e minúsculas

Alguns mecanismos de autenticação são "*case sensitive*", ou seja, tratam letras maiúsculas e minúsculas como caracteres distintos. Senhas que envolvem estas duas características são mais seguras.

Criar senhas de forma que se utilize as duas mãos para digitar

Deve-se criar senhas com letras bem distribuídas pelo teclado, de forma que se tenha de utilizar as duas mãos para digitá-la.

> *Por exemplo, se utilizar como senha a combinação **15xadrez**, poderá digitá-la apenas com a mão esquerda. No entanto, se utilizar **30almofadas**, terá que digitar usando as duas mãos.*

Usar regras para criar suas senhas e não esquecê-las

Ao criar senhas com base em regras, apenas precisa-se lembrar das regras para saber qual é a senha corresponde a cada serviço.

COMO PROTEGER AS SENHAS

Guardar as senhas na mente

Deve-se evitar escrever a senha em pedaços de papel, agendas, arquivos electrónicos desprotegidos ou em qualquer meio que possa ser acedido por outra pessoa.

Não usar a opção de "lembrar senha" em computadores públicos

Em computadores públicos ou do escritório, não se deve utilizar a opção de "inserir senhas automaticamente", "lembrar senha" ou equivalente que muitos *sites* e navegadores oferecerem.

Sempre clique em Sair, *Logoff* ou equivalente

Não se deve contentar em fechar o navegador ao sair de determinado *site*. Esse procedimento é seguro na maioria das vezes, no entanto, em alguns casos, a simples reabertura da página pode disponibilizar o conteúdo sigiloso (conta de e-mail, por exemplo) ser exibido novamente. Para garantir que isso não aconteça é clicando nos *links* ou botões com os dizeres "Sair", "*Logoff*", "*Sign out*" ou equivalente, sempre.

Não utilizar senhas importantes em computadores públicos ou redes desconhecidas

Deve-se evitar aceder serviços muito importantes em computadores públicos (conta bancária, por exemplo). Caso seja inevitável, deve-se verificar se o *site* oferece recursos de segurança (como protecção por SSL). Também evitar usar senhas em redes WI-FI desconhecidas ou públicas.

Trocar a senha periodicamente

É muito importante trocar as suas senhas periodicamente, pelo menos a cada 45 dias. Ao proceder assim, impede-se, por exemplo, que uma pessoa que capturou a senha e esteja a usar discretamente uma conta em um serviço qualquer continue a fazê-lo.

Não usar a mesma senha para vários serviços

Para cada serviço, deve-se utilizar uma senha diferente. Caso, uma pessoa capture a senha apenas terá acesso a esse serviço.

Cuidado com e-mails ou sites falsos que pedem a senha

Um dos golpes mais frequentes na internet são e-mails que direccionam para *sites* que se passam por páginas de bancos, correio electrónico, redes sociais, entre outros, imitando inclusive o visual dos serviços originais. Se o usuário não perceber que está aceder um *site* falso, vai acabar entregando a sua senha e outros dados para um infractor. Assim deve-se ficar sempre atento aos detalhes que permitem identificar e-mails ou sites falsos, como endereços não relacionados com o serviço, erros ortográficos grosseiros e solicitações suspeitas (solicitação de cadastro, por exemplo).

7. Criptografia

Conjunto de técnicas matemáticas para rescrever uma mensagem (ou arquivo) de forma incompreensível por parte das pessoas não autorizadas. A palavra Criptografia vem do grego "*Kryptós*", "oculto" e "*Graphein*", "escrita", portanto "escrita oculta (ou secreta)". O objectivo da criptografia é permitir que um conjunto limitado de entidades, tipicamente duas, possam trocar informação que é ininteligível para terceiros. A criptografia deve ser possível de reverter para os usuários que possuem o código específico para esse fim (chave criptografada).

A criptoanálise é a arte ou ciência de violar informação criptografada ou sistemas criptográficos. O desenvolvimento de técnicas criptográficas motiva, naturalmente, o desenvolvimento de métodos de criptoanálise para contrariar o propósito das criptografias. Estes métodos destinam-se a descobrir, através dos mais variados processos, os elementos ocultados através da criptografia ou as técnicas ou os aspectos particulares usados para efectuar (algoritmos, chaves, entre outros).

A criptologia é o ramo do saber que se dedica ao estudo da criptografia e da criptoanálise. Um criptólogo é alguém que se dedica a estudar problemas tanto de criptografia como de criptoanálise. Na prática esse estudo é em parte indissociável, porque o desenho ou o uso correcto de técnicas criptográficas pressupõe que exista alguma noção dos riscos de criptoanálise das mesmas.

O objectivo da criptografia é transformar uma mensagem em um texto codificado, garantindo a confidencialidade da informação contida. O principal uso da criptografia é a troca segura de informações sigilosas, como senhas de usuários. Actualmente, existem dois métodos de criptografia: A criptografia simétrica e a criptografia assimétrica.

O recurso a tecnologias de cifras torna-se fundamental. Estas não são mais que técnicas e aplicações para a transformação de informação num formato que torna impossível de ler sem um conhecimento especial. As tecnologias de cifra disponibilizaram os meios para assegurar confidencialidade, integridade da informação, identificação e não-repudio [Schneier, 1969].

Por **Confidencialidade,** entende-se o manter seguro o conteúdo de uma mensagem evitando que possa ser acedido por alguém não autorizado para o fazer, tornando-se dessa forma conhecedor do mesmo.

Por **Integridade,** entende-se a detenção de alterações, como sejam edições ao conteúdo, eliminação parcial ou qualquer outra modificação, por pessoas não autorizadas a fazê-lo.

Não-repudio, consiste em garantir que não é possível que alguém repudie ou negue responsabilidade para uma mensagem ou acção.

8. Politicas de Criptografia

Criptografia é uma medida que uma organização empregar se, por exemplo, dados confidenciais estiverem envolvidos. O uso de criptografia deve ser cuidadosamente considerado e definido em um documento de politicas. Esse documento de politicas é a base para determinar como aplicar a criptografia dentro dos sistemas de informação da organização. O documento deve conter ao menos as seguintes informações:

- Para que a organização use criptografia. Um aspecto particular a considerar antes de usar a criptografia são as limitações legais na troca de informação cifradas com organizações ou departamentos em outros países. Isso é importante, visto que em alguns casos não é permitido usar certos tipos de criptografia ou transportar softwares criptográficos através das fronteiras de países;
- Que tipo de criptografia a organização usa, e em quais aplicações. Isso é importante para limitar qualquer problema proveniente de aplicações ou algoritmos criptográficos incompatíveis. Ao ter uma

politica corporativa e ao controlar a sua implementação, esses problemas de compatibilidade podem ser reduzidos ao mínimo;

- Controlo e gestão de chaves. A base de todo o sistema criptográfico são as chaves;
- Normalmente os algoritmos de um sistema criptográfico são públicos e a força do sistema está baseada na força das chaves e na habilidade de a organização evitar que essas chaves caiam em mãos erradas. É, portanto, primordial para uma organização possuir politicas claras e rigorosas sobre como gerir essas chaves;
- *Backup*. Ao fazer *backup* de dados cifrados, é importante determinar como os dados originais podem ser acedidos quando requerido. Isso é especialmente importante quando a chave é perdida ou comprometida, o que significa que usuários não autorizados obtiveram acesso a chave; e
- Controlo. Isso descreve a forma como a aplicação de um material criptográfico é tratada pela organização e quais medidas estão em vigor para limitar o uso indevido. Tal uso indevido pode incluir funcionários deliberadamente criptografando dados, sem autorização, deixando a empresa sem acesso às informações.

9. Criptografia baseada em chaves

Uma chave é um valor matemático que determina como uma mensagem em texto plano será criptografada para produzir um texto cifrado, e ela também é necessária para que possamos recuperar a mensagem original.

A segurança de um sistema de criptografia deve residir em suas chaves, e os algoritmos devem ser sempre de conhecimento público.

A chave é um número secreto usado por um algoritmo de criptografia para alterar o texto plano e convertê-lo em texto cifrado, e é gerada aleatoriamente.

Se mesma chave for usada para encriptar e desencriptar os dados, temos uma chave simétrica, no caso de uso de chaves diferentes para encriptar e desencriptar os dados, temos uma chave assimétrica.

A chave é necessária pois manter o algoritmo em segredo não é efectivo, os invasores invariavelmente quebram o algoritmo (descobrem seu funcionamento).

As técnicas baseadas em chave, orientadas para códigos binários, funcionam com um algoritmo conhecido, parametrizado com chave. Fundamenta-se na complexidade da determinação da chave de decifrar. O princípio básico destas técnicas é como é como se descreve abaixo:

- Existem chaves *K1* e *K2* e funções de cifrar *C* e de decifrar *D*, tais que:
  - *C(K2,m)=x ; D(K1,x)=m ; D(K1,C(K2,m))=m*
- *M* representa a mensagem em claro e *x* a mensagem cifrada;
- Dado *x*, deve ser muito difícil recuperar *m*, não sabendo *K1*; dado *m* e *x=C(K2'm),* deve ser muito difícil recuperar *K2*; dado *Ki*, deve ser muito difícil recuperar *Kj*.

Características de uma chave

Comprimento da chave: número de *bits* na chave (às vezes *bytes*).

Espaço de chaves: colecção de todos os valores matemáticos possíveis que tenham o mesmo comprimento de uma chave. Na prática, é o tamanho da chave, medido em *bits*.

Uma chave de comprimento não gera um espaço de chaves de *2n* valores distintos. Uma chave de 64 *bits,* portanto tem um intervalo de 0 a 264 combinações possíveis. Cada *bit* adicional dobra o tempo necessário para quebrar a chave, ou seja, chaves maiores dificultam o trabalho de um invasor.

Gestão de chaves

A gestão de chaves é uma parte importante de qualquer sistema criptográfico. Chaves criptográficas deve ser protegidas contra alterações, perda ou destruição, uma vez que qualquer uma dessas acções pode resultar na impossibilidade aceder aos dados. Não que os dados sejam realmente perdidos, no entanto sem a chave apropriada o dado não esta disponível em uma forma legível. Uma boa gestão de chaves é essencial para manter a confidencialidade dos dados. Como a perda de chave criptografada é comparável à perda do dado, a gestão de chave também é importante para a disponibilidade do dado. Adicionalmente, dependendo do suso da criptografia em uma organização, a divulgação não autorizada da chave pode ter implicações severas na integridade do dado.

Além disso, quando a criptografia é usada para a confidencialidade dos dados, chaves secretas e pessoas devem ser protegidas contra divulgações não autorizadas, uma vez que isso é potencialmente uma brecha na confidencialidade da informação. Como as chaves são as bases para qualquer sistema criptográfico, o equipamento que é utilizado para gerar, armazenar e arquivar chaves deve ser protegido fisicamente. Uma parte da gestão das chaves é o registo dos pares de chaves e de quem os usa. Ao utilizar um sistema de criptografia assimétrica, pares de chaves são usados para determinar a autenticidade e o não repúdio da mensagem, então o registo deve abranger quais pares foram emitidos para quem e quando. Outros tópicos que devem ser tratados na gestão de chaves incluem por quanto tempo as chaves ficaram válidas e o que deve ser feito se as chaves forem comprometidas.

Ao usar criptografia para proteger a informação armazenada no equipamento, é um alto risco usar as mesmas chaves para todos os equipamentos, ou uma grande parte delas, dentro de uma organização. Se alguma dessas chaves se tornar conhecida fora da organização, então o equipamento (tal como discos rígidos cifrados em *laptops*) terá que receber novas chaves, uma vez que, potencialmente, todos os dados armazenados nesse dispositivo ficaram comprometidos pela perda da chave. Isso pode ser uma operação muito cara, que deve ser realizada bem rapidamente e afim de prevenir uma brecha na confidencialidade da informação.

É fácil ver que a força de um sistema criptográfico está directamente relacionada à qualidade da gestão de chaves. Isso pode ser ilustrado pelo seguinte exemplo. Imagine um algoritmo tecnicamente perfeito que não pode ser quebrado, tal como um cadeado à prova de roubo. É muito fácil para um ladrão esse cadeado se ele tiver acesso à chave. Proteger a chave de roubo, duplicação ou destruição é essencial para que o cadeado opere de acordo com o requisito de manter pessoas não autorizadas do lado de fora e permitir que pessoas autorizadas abram a porta.

10. Criptografia Simétrica

Consiste no uso de uma única chave que é partilhada entre o emissor e o receptor, esta chave é utilizada para cifrar uma mensagem, utilizando-se um algoritmo especifico para o efeito. A mesma chave é posteriormente utilizada para decifrar a mensagem, com utilização do respectivo algoritmo para decifar.

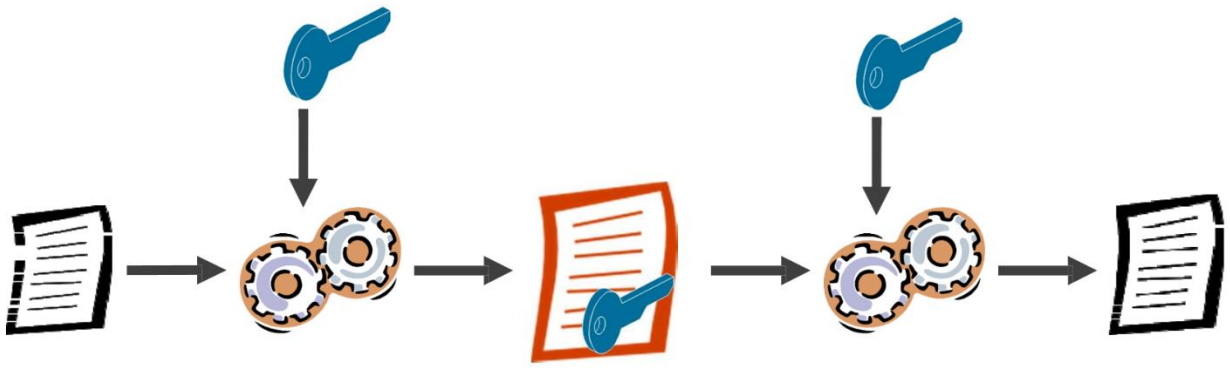


Figura – Criptografia simétrica

Um requisito fundamental neste tipo de técnicas criptográficas é a obrigação de a chave a ser utilizada ter de ser trocada entre as partes intervenientes, forma segura, mantendo a confidencialidade e a integridade. Frequentemente, as chaves são trocadas recorrendo-se a canais de comunicação diferentes daquele que posteriormente será utilizado para a transmissão das mensagens cifradas.

A criptografia simétrica é também muitas vezes denominada de criptografia de chave partilhada ou secreta.

Existe uma única chave *K* e funções de cifrar *C* e de decifrar *D*, tais que:

$C(K,m)=x\ ;\ D(K,x)=m\ ;\ D(K,C(K,m))=m$

Onde *m* representa a mensagem em claro e *x* a mensagem cifrada.

As cifras simétricas podem ser categorizadas em cifras sequenciais ou cifras por blocos. A cifra sequencial tem por finalidade, como alias como o seu nome indica, cifrar sequências de *bits* em tempo real. Estas cifras são frequentemente utilizadas para a codificação de transmissões áudio ou vídeo.

A sua implementação é quase exclusivamente conseguida em *hardware*, já que a sua eficiência computacional tem de ser extremamente elevada. A função cifrar é aplicada *bit* a *bit*, de modo diferente em cada *bit*. Tal significa que se, se quiser cifrar não apenas um bit, mas uma sequência de *bits*, então temos de possuir uma sequência de chaves de igual cumprimento. Esta sequência é gerada por um algoritmo apropriado, a que se dá o nome de gerador de chaves, e que é controlado por uma chave de controlo. As várias cifras sequenciais distinguem-se apenas pela forma do gerador de chaves.

Embora as cifras de chave simétrica sejam usualmente rápidas de computar, apresentam a grande desvantagem de se a chave for quebrada num dos extremos do canal de comunicação, então todo o canal fica comprometido. E tal pode ocorrer num dos extremos sem hipótese de atempadamente se poder informar ao outro extremo.

Um exemplo deste tipo de cifra é o *Data Encryption Standard* (DES), criado em 1977. Outros exemplos são o triple-DES, IDEA, RC2 e RC4. O DES é um algoritmo de chave única, que cifra blocos de 64 *bits* com uma chave de 56 *bits*. Após uma permutação inicial de *bits*, um bloco de texto em claro passa por 16 iterações de uma função complexa e por uma permutação final que gera o bloco cifrado.

A criptografia simétrica apresenta algumas contrariedades, não obstante a enorme vantagem da velocidade que permite, o que é particularmente interessante para cifar grandes quantidades de informação.

Para utilizar DES, ou qualquer outro sistema de cifra de chave única para cifrar comunicações, as duas partes envolvidas no processo têm primeiramente de acordar numa chave secreta de sessão, que será utilizada para cifar todas as comunicações em ambas as direcções. Ao processo de estabelecimento de chave de sessão chama-se troca de chaves, negociação ou distribuição.

Os principais problemas deste tipo de cifra podem ser resumidos nos seguintes pontos:

- Se a chave é perdida, todo o canal esta comprometido;
- Convém mudar frequentemente de chave, diminuindo-se dessa forma o risco de comprometimento da mesma; e
- A distribuição de chaves é cifrada, pois se houver lugar ao comprometimento da chave no momento da chave no momento em que a mesma é distribuída, então todas as mensagens posteriores que recorram à sua utilização podem ser decifradas por quem interceptou.

11. Criptografia Assimétrica

Consiste no recurso a uma chave que é utilizada para cifrar uma mensagem, utilizando-se um algoritmo específico para o efeito. Outra chave diferente é posteriormente utilizada para decifrar a mensagem, com utilização do respectivo algoritmo para decifrar.

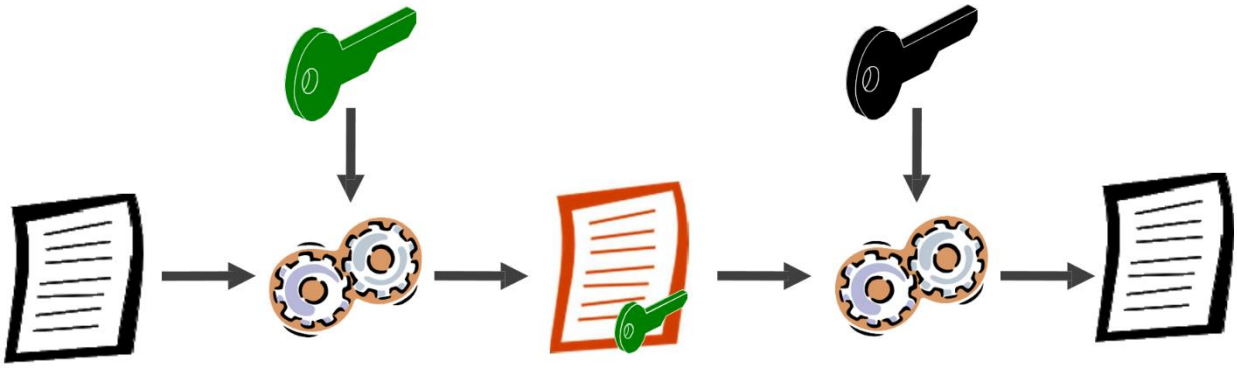


Figura – Criptografia assimétrica

Cada um dos extremos do canal de comunicação conhece uma chave que só pode ser utilizada com um objectivo bem determinado, ou seja, para cifrar num dos extremos e para decifrar no outro. Mesmo conhecendo-se uma das chaves, não é possível determinar-se a outra.

A chave de cifrar é pública, no sentido em que qualquer utilizador que pretenda, pode conhecer, e a chave de decifar é secreta e exclusivamente do conhecimento de quem decifra.

Existem chaves *Ks* (chave secreta) e *Kp* (chave publica) e funções de cifrar *C* e de decifrar *D*, tais que:

$$C(Kp,m)=x\ ;\ D(Ks,x0=m\ ;\ D(Ks,C(Kp,m))=m;\ C(Kp,D(Ks,m))=m$$

Em que *m* representa a mensagem em claro e *x* a mensagem cifrada.

Assim, *C* e *D* são funções equivalentes; pode-se cifrar/decifar com a chave pública ou com a privada.

Este tipo de criptografia é mais lento que a criptografia simétrica, exigindo mais poder computacional. Um exemplo de criptografia assimétrica é o algoritmo *Rivest-Shamir-Adleman* (RSA), criado em 1978. Outros exemplos são o DAS e GPG.

As técnicas assimétricas garantem a confidencialidade, pela utilização das chaves pública e secreta. O destinatário das mensagens públicas a sua chave de cifrar, que serve exclusivamente para esse fim, e guarda a chave secreta de decifrar, não a divulgação.

A criptografia assimétrica tem alguns problemas, de onde salientam-se a fragilidade da base de dados de chaves publicas, sujeita a penetração por um intruso e substituição da chave do utilizador *X* pela dele. Tal evita-se recorrendo a autoridades certificadoras - AC (CA- *Certification Authority*), que funcionam também como centros de distribuição de chaves (KDC – *Key Distribution Center*). A missão da das autoridades de certificação é verificar a verdadeira identidade dos indivíduos, ligando a mesma à chave pública e verificando que esse mesmo individuo possui a chave privada correspondente. Aos ficheiros que são assinados digitalmente pela autoridade de certificação e através dos quais certificam a associação entre os indivíduos e as suas chaves publicas chamamos Certificados Digitais.

12. Hash

A função *Hash* é qualquer algoritmo que mapeie dados grandes e de tamanho variável para pequenos dados de tamanho fixo. Por esse motivo, as funções *Hash* são conhecidas por resumirem o dado. Ou seja, é uma função criptográfica que gera uma saída de tamanho fixo (geralmente 128 a 512 *bits*) independentemente do tamanho da entrada. A esta saída se denomina de *hash* da mensagem (ou documento ou o que quer que seja a entrada). Para ter utilidade criptográfica, a função de *hashing* deve ter as seguintes características:

- **Unidirecionalidade:** conhecido um resumo *h(M)*, deve ser computacionalmente impossível encontrar *M* a partir do resumo;
- **Compressão:** a partir de uma mensagem de qualquer longitude, o resumo *h(M*) deve ter uma longitude fixa. O normal é que a longitude de *h(M)* seja menor do que a da mensagem *M*;
- **Facilidade de cálculo:** deve ser fácil calcular *h(M)* a partir de uma mensagem *M*;
- **Difusão:** o resumo *h(M)* deve ser una função complexa de todos os bits da mensagem *M*: se, se modifica um só *bit* da mensagem *M*, o *hash h(M)* deveria mudar a metade dos seus *bits* aproximadamente;
- **Colisão simples:** será computacionalmente impossível, conhecido *M*, encontrar outro *M'* tal que *h(M) = h(M')*. Isto se conhece como resistência débil às colisões; e

- **Colisão forte:** será computacionalmente difícil encontrar um par (*M, M'*) de forma que *h(M) = h(M')*. Isto se conhece como resistência forte às colisões.

Em um primeiro momento é gerado um resumo criptográfico da mensagem através de algoritmos complexos que reduzem qualquer mensagem sempre a um resumo de mesmo tamanho. A este resumo criptográfico se dá o nome de ***hash***.

Os principais algoritmos são:

- **MD2 *Message Digest Algorithm RDA-MD2***, definido na RFC 1423.

  Desenhou-se para computadores com processador de 8 *bits*, e hoje quase não se utiliza. Conhecem-se ataques a versões parciais de MD2.

- **MD4**

  Foi introduzido com o objectivo de que fosse uma função rápida mas já se demonstrou que não é seguro. Demonstrou-se que era possível achar colisões para MD4 em menos de um minuto utilizando um Computador simples.

- **MD5, *Message Digest Algorithm RDA-MD5***, definido na RFC 1321.

  É uma versão melhorada de MD4. Pelo momento é considerado seguro, ainda que se recomende que, "por via das dúvidas", se actualize qualquer produto que o utilize a outros algoritmos como SHA-1.

Há que destacar que estes algoritmos se encontram no domínio público e, porém, não se vêem afectados por problemas de patentes.

- **SHA-1*, Secure Hash Algorithm***, definido no NIST-FIPS 180-1.

  É muito similar, no seu modo de operação, com o MD5. Este algoritmo é ligeiramente mais lento do que MD5, mas a maior longitude do resumo da mensagem o faz mais seguro frente à procura de colisões usando a força bruta.

Dessa forma, as funções *Hash* são largamente utilizadas para buscar elementos em bases de dados, verificar a integridade de arquivos baixados ou armazenar e transmitir senhas de usuários.

Uma vez que o *hash* tem tamanho fixo, deduz-se que o número de funções *hash* possíveis que podem ser geradas é limitada e em contrapartida, o número de mensagens que podem ser geradas e enviadas ser infinitas. De fato, é impossível impedir que mensagens diferentes levem a um mesmo *hash*. Quando se encontram mensagens diferentes com *hashes* iguais, é dito que foi encontrada uma colisão de *hashes*. Um algoritmo onde isso foi obtido deve ser abandonado.

As funções de *hash* estão em constante evolução para evitar que colisões sejam obtidas. Cabe destacar que a colisão mais simples de encontrar é uma aleatória, ou seja, obter colisões com duas mensagens geradas aleatoriamente, sem significado real. Quando isto ocorre os estudiosos de criptografia já ficam atentos, porém para comprometer de maneira imediata a assinatura digital seria necessário obter uma mensagem adulterada que tenha o mesmo *hash* de uma mensagem original fixa, o que é teoricamente impossível de ocorrer com os algoritmos existentes hoje.

A função de *Hash*, possui vários algoritmos (DSA, RSA, Elgamal, HMAC, entre outros). Destacar o HMAC que é o resultado do trabalho realizado no desenvolvimento de um MAC derivado de funções criptográficas de *hash*. O HMAC é um grande resistente a ataques de criptoanálise, pois usa o conceito de *Hashing* duas vezes. O HMAC consiste em benefícios duplos de *Hashing* e MAC e, portanto, é mais seguro do que qualquer outro código de autenticação.

Tem como objectivos:

- Ser unilateral, ou seja, fácil de gerar saída a partir da entrada, mas complexo ao contrário;
- Ser menos afetado por colisões do que as funções *hash*;
- O HMAC reutiliza os algoritmos como MD5 e SHA-1 e verifica a substituição das funções *hash* incorporadas por funções *hash* mais seguras, caso seja encontrado; e
- O HMAC lida com as Chaves de maneira mais simples.

O funcionamento do HMAC inicia com a obtenção de uma mensagem M contendo blocos de *bits* de comprimento *b*. Uma assinatura de entrada é preenchida à esquerda da mensagem e fornecida como entrada para uma função *hash* que nos dá um resumo de mensagem temporário MD '. MD 'novamente é

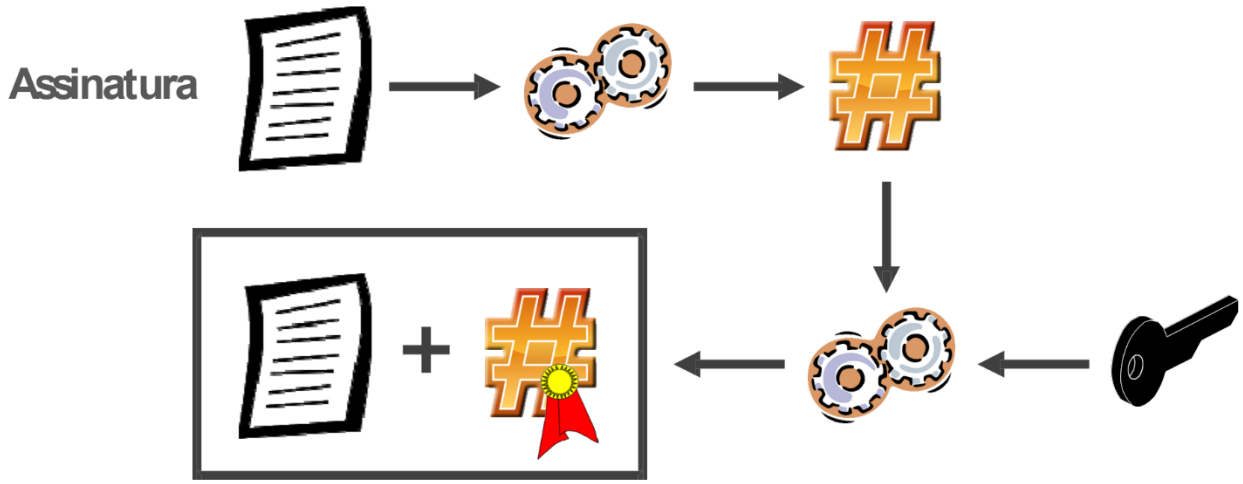
anexado a uma assinatura de saída e o todo é aplicado a uma função *hash* novamente, o resultado é nosso resumo de mensagem MD final.

13. Assinatura Digital

Consiste num código digital que é anexado a uma mensagem transmitida por meios electrónicos e que permite a identificação unívoca do emissor e garante a integridade da mensagem. A assinatura digital é particularmente importante no comércio e negocio electrónico e constitui-se como uma componente chave em sistemas de autenticação.

Na prática consistem na criação de um *hash* obtido por uma função *one-way*, que depois é cifrado com a chave privada do emissor da mensagem. Este *hash* cifrado é adicionado à mensagem original e o resultado enviado para o destinatário da mesma. Este separa a assinatura da mensagem, passa-a pela mesma função de *one-eay hash* e compara com o *hash* que obteve pela decifração da assinatura com a chave pública do emissor. Se forem iguais, então a mensagem não foi alterada durante a transmissão.

A utilização da assinatura garante um conjunto de propriedades que interessa referir, nomeadamente: não-forjamento, autenticidade, não-reutilização, não-repudiação e integridade do documento. O não-forjamento é assegurado pelo facto de quem assinou o fez deliberadamente, já que utilizou inclusivamente a sua chave privada para o efeito. A autenticidade garante que quem assinou é identificável, pois se conseguirmos decifrar a assinatura com determinada chave pública, então sabemos que podemos identificar o dono da mesma. A não-reutilização garante que a assinatura não pode ser utilizada num outro documento, pois o *hash* produzido seria garantidamente diferente, o que significaria que ou a mensagem teria sido alterada na transmissão ou a assinatura é falsificada. O não-repudio garante que quem assinou não pode negar que o fez. A integridade garante que o documento não é alterável depois de assinado. Se for desejável que o conteúdo da mensagem tenha também algum grau de confidencialidade, então este deve ser cifrado com a chave pública do destinatário.



Os esquemas de encriptação assimétricos garantem sigilo na comunicação entre duas partes, mas chaves públicas podem ser usadas também para garantir o não-repúdio (ou irretratabilidade) de documentos: *por exemplo, se Alice usa sua chave privada para criar um documento, qualquer um de que tenha sua chave pública poderá verificar que realmente Alice publicou aquele documento (e Alice não poderá posteriormente negar que o fez).*

Para assinar com criptografia simétrica, torna-se necessária a existência de um arbitro, que partilha com cada utilizador uma chave secreta. Este árbitro vai desempenhar um papel central em todo o processo.

O emissor da mensagem cifra a mesma com recurso à chave secreta que partilha com o árbitro e envia-a a este. O árbitro decifra a mensagem e volta a cifrá-la, utilizando a chave secreta que partilha com o destinatário, juntamente com uma cópia da mensagem original cifrada e certificado de validade e envia-a ao destinatário. O destinatário recebe a mensagem, decifra-a com a chave secreta que partilha com o árbitro, podendo ver a mensagem e o certificado que vem em anexo.

O certificado SSL é essencial para garantir uma comunicação de dados segura, e para evitar que seu domínio seja marcado como inseguro (sem HTTPS). Existem serviços que oferecem certificados gratuitos como o Let's Encrypt, contudo, não fornecerem garantias quanto à confiabilidade dos dados.

Funcionamento das assinaturas (documentos electrónicos)

É usada a assinatura digital, um recurso electrónico capaz de criptografar o conteúdo do seu documento. Eles utilizam chaves criptográficas, um conjunto de bits baseados em determinado algoritmos, capaz de cifrar e decifrar informações. Utilizamos chave simétrica (simples, e ambos o receptor e o emissor da mensagem podem utilizar as mesmas chaves) ou assimétrica (pública e privada: o dono da chave privada deve disponibilizar a chave pública para quem estiver autorizado a ter acesso à informação. Uma chave estará associada a outra). Observe:

- **O emissor deve ter:** documento + chave privada para codificar a informação e enviar para o destinatário;
- **O receptor usará:** sua chave pública para decifrar o documento; e
- Se o documento tiver sido alterado ou sua assinatura deformada, ele se tornará invalido.

Sobre a definição de chave assimétrica, elas são as que correm pouco risco de fraudes e são suas chaves públicas as utilizadas em assinaturas digitais. Uma Autoridade Certificadora, entidade que dá o poder a uma pessoa de adquirir seu certificado, por sua vez, trabalha com duas chaves: a **chave privada e a chave pública**. Nesse esquema, uma pessoa ou uma organização deve utilizar uma chave privada (sigilosa e individual) para codificar a informação e disponibilizar uma chave pública a quem for mandar informações a ela, usada pelo receptor da informação para o processo de decodificação. Ambas as chaves são geradas de forma conjunta; portanto, uma está associada a outra.

Uma das principais implementações de assinaturas com recurso a criptografia assimétrica é o PGP (*Prety Good Privacy*), desenvolvido por Phil Zimmermann [Zimmermann, 1995] e gratuitamente disponível em várias versões. O PGP é correntemente utilizado na protecção de mensagens de correio eletrónico e de arquivos. Implementa um mecanismo de cifra baseado em sistema de chave pública e, em algumas versões, utiliza um mecanismo híbrido, baseado em sistema de chave pública para troca de informação de controlo e sistema de chave secreta para a troca de dados em volume.

O PGP assegura a confidencialidade e autenticação e opera segundo princípios estabelecidos e aceites, tendo-se transformado quase num *standard* de facto [PGP]. O sistema de autenticação funciona com base em cadeia de confianças mútuas. *Por exemplo, supomos que Alice não conhece Bernardo, no entanto*

ambos conhecem Catarina e a sua chave pública. Assim, Catarina pode assinar certificado de chave pública de Alice e de Bernardo, dando a Alice o certificado de chave de Bernardo, e a Bernardo o certificado da chave de Alice. Assim, Alice e Bernardo serão mutuamente apresentados.

Uma implementação de PGP assegura um conjunto de funcionalidades indispensáveis ao funcionamento do sistema, em particular cifrar, assinar, cifrar e assinar, guardar arquivos com criptografia convencional e decifrar e/ou verificar assinaturas.

14. Infra-estrutura de Chave Publica (*Public Key Infrastructure* – PKI)

Embora a criptografia assimétrica também seja referida como criptografia de chave pública, não é a mesma coisa que a infra-estrutura de chave pública (*Public Key Infrastructure* – PKI). PKI é baseada em criptografia de chave pública e inclui muito mais do que somente a criptografia. Uma característica de uma PKI é que, através de acordos, procedimentos e uma estrutura organizacional, ela provê garantias referentes a quais pessoas ou sistemas pertencem a uma chave pública específica. Uma infra-estrutura de chave pública é frequentemente gerenciada por uma autoridade independente e confiável.

A força de uma PKI depende, em grande medida, de aspectos não técnicos. A forma como o usuário obtém sua chave privada, por exemplo, é uma pedra angular na confiança que outras pessoas têm na solução de PKI, mesmo se tecnicamente elas usarem os mesmos algoritmos a tamanhos de chave. Uma PKI em que os usuários podem obter uma chave privada solicitando-a por e-mail, usando, por exemplo, o Gmail, é inerentemente menos confiável para identificar uma pessoa com base em sua chave pública do que um sistema onde os usuários têm de reportar a uma mesma e se identificar, por meio de um passaporte, antes de receber uma chave privada.

Não-repúdio é a garantia de que alguém não pode negar algo. Tipicamente, o não-repúdio se refere à habilidade em assegurar que uma parte de um contracto, ou de uma comunicação, não pode negar a autenticidade de sua assinatura em um documento ou o envio de uma mensagem que originou.

Repudiar significa negar. Por muitos anos, as autoridades têm procurado tornar o repúdio impossível em algumas situações. Pode-se enviar uma correspondência registada, por exemplo, de forma que o destinatário não possa negar que a carta foi entrega. De forma similar, um documento legal tipicamente requer testemunhas de sua assinatura, para que a pessoa que assina não possa negar tê-lo feito.

Na internet, uma assinatura digital é utilizada não só para assegurar que um documento (ou mensagem) tenha sido assinado electronicamente pela pessoa que supostamente assinou o documento, porém, também para garantir que uma pessoa não possa negar mais tarde que forneceu a assinatura, visto que uma assinatura digital só pode ser criada por uma pessoa. Uma PKI é uma solução para alcançar o não-repúdio. A ISO define o não-repúdio como uma habilidade de provar a ocorrência de um evento ou um evento ou uma acção reivindicada e suas entidades originarias, afim de solucionar disputas sobre a ocorrência ou não de evento ou acção e o envolvimento de entidades no evento.

Autoridade Certificadora (AC)

A Autoridade Certificadora é a entidade mais importante de uma estrutura de PKI. Ela é responsável por gerar e assinar os certificados para os usuários e serviços que desejam utilizar a infra-estrutura de chaves públicas. E revogar certificados caso seus donos infrinjam as políticas estabelecidas pela autoridade. Ela é uma entidade confiável, que se responsabiliza pela autenticação, ou seja, de que os usuários e serviços a ela vinculados são realmente o que eles dizem ser. Sempre que um usuário recebe um certificado ao utilizar um serviço e desejar verificar a sua autenticidade, ele pode se comunicar com a autoridade certificadora e averiguar se o certificado está sendo utilizado correctamente, se ele ainda é válido e quais são os limites de utilização do certificado.

Os certificados podem ser emitidos através da própria Internet mediante o cadastro da entidade na página Web da autoridade, ou através de dispositivos de armazenamento seguros, de forma *off-line*. Dependendo da política empregue na autoridade, os registos de novos certificados podem ser efectuados através da própria Internet, porém, firmas mais sérias de autenticação podem requerer uma visita física ao representante da autoridade, onde quem requisitou o certificado precisa se registar manualmente, tirar retractos, e comprovar sua verdadeira identidade através de um cartão de identidade ou um passaporte. A figura abaixo proporciona uma visão geral dos componentes das entidades de uma PKI.

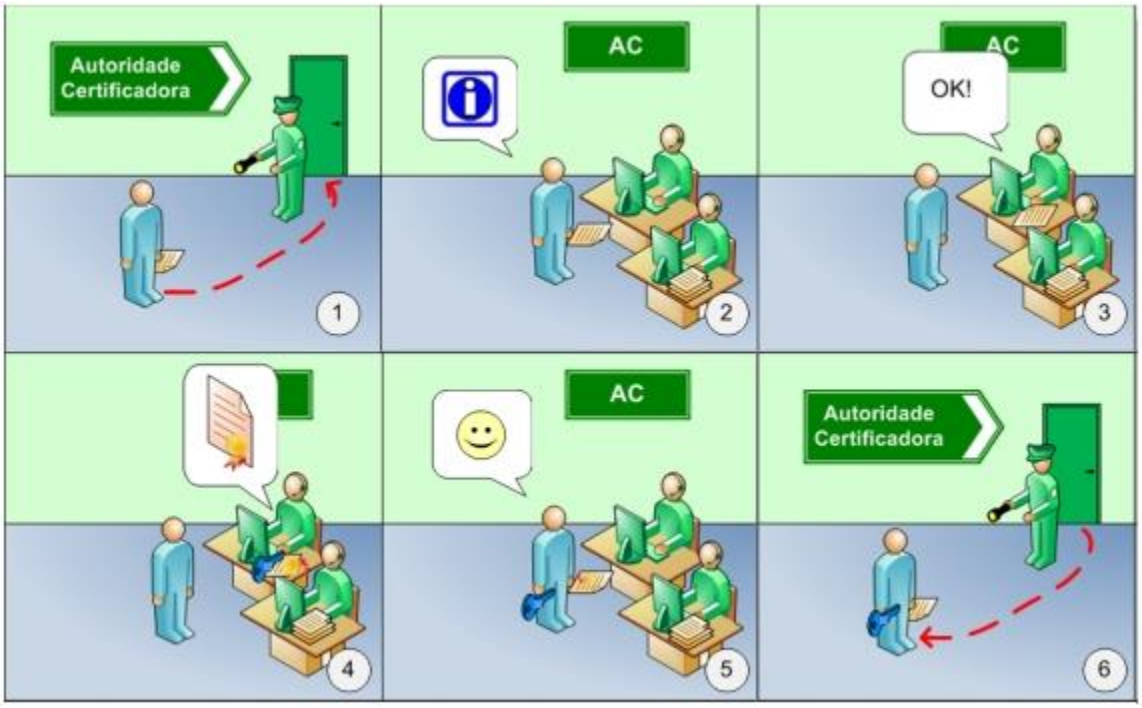


Figura – Procedimento de obtenção de um certificado.

1- Usuário se dirige a autoridade certificadora.
2- Usuário entrega uma requisição de certificado para a autoridade, repassa suas informações e se registra com a autoridade.
3- Autoridade verifica com sucesso a idoneidade do usuário.
4- Autoridade emite o certificado do usuário, de acordo com suas políticas e restrições e lhe entrega sua chave privada.
5- Usuário concorda com o certificado recebido e com a chave recebida.
6 – Usuário pode utilizar o certificado e a chave.

Autoridade de Registo (AR)

A autoridade de registo é uma entidade opcional. Ela pode actuar como um intermediário entre os assinantes de um serviço de certificação e a autoridade certificadora. Desta forma, a autoridade de registro recebe os pedidos de certificados e as informações a respeito do assinante e as repassam para a autoridade certificadora. Em alguns casos, a autoridade certificadora pode delegar a responsabilidade alguns tipos de certificados para a autoridade de registo, de forma que as mensagens por ela assinadas possuem o mesmo valor de uma mensagem assinada directamente pela autoridade certificadora. Uma única autoridade certificadora pode operar conjuntamente com diversas autoridades de registro.

Assinante

O assinante é a entidade que deseja receber um certificado da autoridade certificadora. Analisando o conteúdo do certificado emitido, podemos verificar o nome do assinante e informações referentes a qual organização ele está vinculado, qual é o escopo daquele certificado, a sua validade, e qual autoridade certificadora o assinou.

Usuário de um serviço protegido por certificados (*Relying Party*)

O *Relying Party* é o usuário que recebeu uma informação assinada digitalmente, ou que deseja utilizar um serviço protegido por um certificado. Este usuário precisa utilizar a infra-estrutura de chaves públicas para verificar a autenticidade desta informação assinada digitalmente e a autenticidade do serviço protegido por um certificado.

Âncora de Confiança (*Trust Anchor*)

Uma âncora de confiança é uma chave pública que um usuário de um serviço protegido por certificados confia para assinar certificados. Em uma cadeia de certificados, o primeiro certificado, que começa a cadeia de certificação, precisa ter sido assinado com esta âncora de confiança.

Repositório

O repositório está intimamente ligado a autoridade certificadora. Dentro dele, estão armazenadas todas as informações referentes aos certificados que já foram emitidos pela autoridade, quais ainda estão em uso, qual o escopo de cada um deles e quais certificados não são mais válidos. Estas informações podem ser apresentadas através de uma página Web.

Operação e gestão da PKI

Para os grupos de trabalho, existem no mínimo, os seguintes papéis privilegiados que devem estar definidos:

Gestão de Topo	• Responsável pelas decisões de gestão e pela nomeação de todos os elementos dos grupos de trabalho.
Administradores de Segurança	• Com a responsabilidade geral pela administração da implementação das políticas e práticas de segurança
Operadores de Registo	• Responsáveis pela aprovação da geração/revogação/suspensão do certificado do titular.
Administradores de Sistema	• Autorizados a instalar, configurar e manter o sistema, mas com acesso controlado a informação relacionada com segurança.
Operadores de Sistema	• Responsáveis por operar o sistema no dia-a-dia, por exemplo: autorizados a efetuar o *backup* e a recuperação do sistema.
Auditores de Sistema	• Autorizados a consultar arquivos e registos de auditoria dos sistemas da PKI.
Custódia	• Armazena com segurança os artefactos sensíveis da PKI e controla o seu levantamento e devolução de acordo com as regras estabelecidas.

Fontes:

- Hintzbergen, J; Hintzbergen, K; Smulders, A; Baars, H (2018). Fundamentos de Segurança da Informação. Rio de Janeiro: Brasport.
- Mamede, Henrique São (2006). Segurança Informática nas Organizações. FCA-Editora Informática.
- Zúquete, André (2013). Segurança em Redes Informáticas. (4ª Ed. Aumentada). FCA-Editora Informática.