SEGURANÇA DOS SISTEMAS DE INFORMAÇÃO – PARTE I

1. SEGURANÇA – CONCEITO

A **segurança de um sistema informático**, isolado ou em rede, pretende minimizar os efeitos que **acontecimentos indesejáveis** possam provocar **no seu funcionamento** ou **na informação** por ele tratada.

Os objetivos a alcançar são diversificados dependendo da ameaça que pretendem combater.

2. SEGURANÇA – OBJETIVOS

Tem como **objetivo** a defesa conta: catástrofes; faltas/falhas previsíveis; atividades não autorizadas.

Desefa contra catástrofes:	Solução:
o Fenómenos naturais; o Degradação do *hardware* computacional.	o Salvaguarda da informação; o Replicação da informação e dos recursos computacionais.

Desefa contra faltas/falhas previsíveis:	Solução:
o Falta de energia; o Falha dos sistemas; o Faltas/falhas nas comunicações.	o Sistemas de alimentação alternativos; o Encaminhamento alternativo/reenvio.

Desefa contra atividades não autorizadas:	Solução:
o Iniciadas por alguém "de dentro"; o Iniciadas por alguém "de fora".	o Acesso e alteração da informação; o Utilização de recursos; o Vandalismo; o Interferência com o normal funcionamento do sistema sem qualquer benefício para o sujeito causador.

3. SEGURANÇA – CONCEITOS

Vulnerabilidade	o Característica de um sistema que o torna sensível a um ataque.
Ataque	o Conjunto de passos que levam à execução de uma ou mais atividade ilícitas normalmente explorando vulnerabilidades.
Risco/ameaça	o Possibilidade de dano resultante de um ataque.
Defesa	o Conjunto de políticas e mecanismo de segurança que visam: **1)** Diminuir as vulnerabilidades de um sistema; **2)** Detetar o mais rápido possível ataques passados ou atuais; **3)** Diminuir os riscos de um sistema.

ASPETOS DE SEGURANÇA

1. AUTENTICAÇÃO

Capacidade de garantir que uma dada entidade é quem afirma ser.

↳ Processo através do qual é validade a identidade de um utilizador, dispositivo ou processo.

↳ Certificados digitais.

2. CONFIDENCIALIDADE

Capacidade de limitar o acesso à informação apenas às entidades (pessoas, processos, máquinas…).

↳ Garantir que os dados não podem ser lidos por entidades que não o destinatário.

↳ Encriptação.

3. INTEGRIDADE

Capacidade de garantir que a informação que está a ser veiculada ou armazenada não é corrompida.

↳ Os dados em trânsito não poderão ser intercetados e alterados.

4. CONTROLO DE ACESSO

Capacidade de impedir o acesso não autorizado a um recurso ou a sua utilização além dos limites autorizados.

↳ Funções de autorização que estabelecem os direitos de utilizadores, grupos e sistemas.

5. NÃO REPÚDIO

Capacidade de impedir que uma entidade envolvida numa transação negue a sua participação no evento.

↳ Após a autenticação dos interlocutores, estes não podem negar ações que tomaram (ex.: após a compra, negar que a efetuou).

6. DISPONIBILIDADE

Capacidade de garantir a disponibilidade dos recursos mesmo na sequência de ataques.

↳ Independentemente de ataques, os recursos chave ficam disponíveis para os utilizadores.

MECANISMOS DE SEGURANÇA

1. ENCRIPTAÇÃO

Permitem a transformação reversível da informação de forma a torna-la ininteligível a terceiros (no emissor).

↳ Estão na base dos aspetos de confidencialidade, autenticação e integridade.

↳ **Desencriptação** – operação inversa da encriptação (no receptor).

2. ASSINATURA DIGITAL

Bloco de texto gerado através de um algoritmo de encriptação aplicado ao documento e a enviar com a chave privada do emissor.

↳ O recetor verifica a validade da assinatura aplicando o mesmo algoritmo com a chave pública do emissor.

↳ Garantem a integridade do documento e a identidade de quem o envia.

↳ Não garantem confidencialidade.

3. CONTROLO DE ACESSO

Conjunto muito variado de mecanismos de autenticação e controlo de acesso a recursos.

↳ Algo que se conhece: passwords (+ usados pela simplicidade).

↳ Algo que se possui: *smart cards*.

↳ Algo que se é: sistemas biométricos (dos + seguros mas também dos + caros).

↳ **Outro tipo de mecanismos de controlo**: listas de acesso; *firewalls*.

4. CERTIFICAÇÃO

Permite atestar a validade de um documento através do envolvimento de uma terceira entidade (entidade de certificação) da confiança do emissor e do recetor na certificação da informação (*trusted third-party*).

↳ **Usado na garantia de integridade de documentos e na autenticação de utilizadores**.

NECESSIDADES DE SEGURANÇA – INTRUSÃO

1. ACESSO NÃO AUTORIZADO

Descoberta de informação de autenticação (nome e *password*) de um dado utilizador, utlizada por outro para aceder aos recursos disponíveis ao primeiro.

↳ Através de:

- Observação da introdução dos caracteres;
- Uso de (*hard*/*soft*)*ware* de monotorização e diagnóstico de redes.

2. ACESSO POR IMITAÇÃO

Fazer com que um dado utilizador ou sistema se comporte como um outro.

↳ Objetivos:
- Obtenção de informação ou recursos críticos;
- Perturbação do funcionamento de serviços.

3. NEGAÇÃO DE SERVIÇO

Objetivo – interrupção ou perturbação de um serviço através de danos caudados nos sistemas que os suportam.

↳ Danos:
- Físicos – destruição de equipamentos ou cablagens;
- Lógicos – eliminação de programas ou dados residentes no disco de um computador.

↳ Danos:
- Disseminação de vírus;
- Geração artificial de grandes volumes de tráfego.

4. ORIGEM DOS ATAQUES

Os atacantes podem ser ***hackers*** ou ***crackers***.

Hacker	o Fanático de computadores; o Gosta de desafios; o Gosta de expor as vulnerabilidades para provar a sua inteligência superior; o Normalmente, não é mal-intencionado.
Cracker	o Mal-intencionado; o Explora as vulnerabilidades em proveito próprio.

POLÍTICAS DE SEGURANÇA

1. POLÍTICA DE SEGURANÇA

- Conjunto formal de regras que devem ser seguidas pelos utilizadores dos recursos de uma organizam;
- Definem detalhadamente as **utilizações permitidas** para os recursos e sistema de comunicações, bem como as **penalizações** em situações de desrespeito.

2. PRINCIPAIS CONTEÚDOS

3. PRINCIPAIS REGRAS PARA UMA BOA POLÍTICA DE SEGURANÇA

1) Ser facilmente acessível a todos os membros da organização;
2) Definir os objetivos da segurança;
3) Definir objetivamente todos os aspetos abordados;
4) Definir a posição da organização em cada questão;
5) Justificar as opções tomadas;
6) Definir as circunstâncias em que é aplicada cada uma das regras;
7) Definir os papéis dos diversos agentes da organização;
8) Especificar as consequências do não cumprimento das regras definidas;
9) Definir o nível de privacidade garantido aos utilizadores;
10) Identificar os contactos para esclarecimento de questões duvidosas;
11) Definir o tratamento das situações de omissão.

SEGURANÇA DOS SISTEMAS DE INFORMAÇÃO – PARTE II

1. SEGURANÇA DA INFORMAÇÃO – INTRODUÇÃO

Um dos motivos do aumento de sistemas informáticos reside na segurança da informação. Essa segurança pode ser vista segundo dois vetores:

- **Prevenir o acesso à informação por terceiros**;
- **Danos eventuais que possam danificar ou destruir essa informação**.

2. PROTEÇÃO CONTRA ACESSO POR TERCEIROS

I. **Palavras-passe (*passwords*)**: conjunto de carateres, normalmente alfanuméricos (letras, números e símbolos) usado para **controlar o acesso** de utilizadores não autorizados à informação.

Categorias de *passwords*	
Password *de rede*	Permite acesso a determinadas áreas de um computador central (servidor) e à informação aí armazenada.
Password *individual de sistema*	Limita o acesso a um único computador e podem impossibilitar o funcionamento do próprio computador.
Password *de programa*	Condiciona o acesso a um determinado programa.
Password *de ficheiros*	Protege um ficheiro ou documento, a nível individual, impedindo a sua abertura, visualização ou impressão.

II. **Encriptação**: consiste na alteração dos dados através de um algoritmo matemático de forma a que estes se tornem ilegíveis sem a respetiva chave de desencriptação. Protege a comunicação entre utilizadores, quer a nível dos documentos, quer das próprias mensagens enviadas por correio eletrónico.

Programas para encriptação
Existem vários programas para realizar este objetivo, muitos deles gratuitos (*freeware*) e disponíveis na Internet.
Um dos melhores será talvez o PGP (*Pretty Good Privacy*) criado por Philip Z. em 1991, convertendo-se depois numa aplicação de cifragem de alta segurança não gratuita.
Existe, no entanto, uma versão *freeware*, PGP Desktop que pode ser utilizada durante 30 dias.

III. **Controlo de acessos remotos**: o **acesso não autorizado** a um computador pessoal tornou-se uma das maiores ameaças à segurança da informação devido à proliferação de redes, sobretudo, da Internet. Os computadores são alvo de ataque de *software* malicioso ou ***malware*** (*malicious software*).
Uma solução de prevenção será instalar e configurar adequadamente um sistema completo de segurança.

Spyware	Obtêm informação sobre o utilizador do computador invadido (ex.: sites visitados para obtenção de informação confidencial).
Vírus	Têm a capacidade de se copiarem a si próprios, "infetando" ficheiros e a memória do computador, realizando ações destruitivas sobre a informação e os seus suportes.
Backdoors	Criam um acesso alternativo ao sistema sem passar pelos mecanismos de proteção e autenticação.
Trojan Horses	Programas "disfarçados" que atuam muitas vezes para abrir *backdoors* e minimizar as proteções do computador.
Key loggers	Registam e enviam para terceiros as teclas pressionadas pelo utilizador com o objetivo de usurpar as *passwords*.
Rootkits	Dissimulam e escondem o facto do sistema ter sido comprometido ao nível da segurança, confundindo-se com aplicações do sistema.
Browser hijack	Altera as propriedades do *browser* da Internet, forçando o direcionamento para um site específico.
Worms	Programas semelhantes a vírus com a particularidade de se propagarem sem se anexarem a um ficheiro.

3. PROTEÇÃO CONTRA DANOS EVENTUAIS

I. **Cópias de segurança**: umas das mais importantes regras de segurança num sistema informático; periódicas; incluindo informação produzida pelo utilizador e programas originais.

- Como **programa para cópia de segurança** podemos utilizar, por exemplo, o Cópia de Segurança e Restauro do Windows 7;
- É habitual os programas de gravação de CD/DVD incluírem programas para cópias de segurança.

Permitem a cópia da informação com compressão, diminuindo assim o espaço de armazenamento necessário. O tipo de suporte a usar depende da dimensão da informação a salvaguardar.

II. **Antivírus**:

Vírus		
Programa ou conjunto de ordens concebido por um programador que	Têm a capacidade de se copiarem a si próprios, "infetando" ficheiros e a memória	Segundo a última referência de meados de 2009 apontava para o facto de se ter

segue as instruções (indesejáveis) para as quais foi criado.	do computador, realizando ações destrutivas sobre a informação e os seus suportes.	ultrapassado a marca de um milhão de diferentes tipos de vírus.

Como se transmitem os vírus?

O processo inicia-se com a infeção de ficheiros. Esses ficheiros, ao serem carregados para a emória, constituem a base da comunicação de informação à distância entre computadores ligados em rede.

O grande desenvolvimento da Internet fez com que se tornasse o principal veículo de transmissão de vírus.

- Envio/receção de correio eletrónico;
- Partilha de ficheiros.

Como proteger o computador/informação?

Devemos adquirir um programa antivírus que possibilite deteção, eliminação e proteção em relação a todos os tipos de vírus, mantendo-o sempre ativo.

Devemos selecionar um antivírus com assistência *online* ou até presencial, pois: é de rápida atualização de ficheiros de dados sobre novos vírus; o acesso a *upgrades* é regular; há assistência técnica para os casos mais "complexos".

4. MANUTENÇÃO PRÉVIA

Fundamental para empresas que possuem um parque informático com alguma dimensão.

↳ Verificação periódica do adequado funcionamento dos vários tipos de *hardware* e *software* assim como da própria organização da informação.

5. GRAVAÇÃO PERIÓDICA DA INFORMAÇÃO

6. UTILIZAÇÃO DO SOFTWARE ORIGINAL

Respeito pelos direitos de autor.

↳ Permite obter suporte técnico e acesso privilegiado a informações sobre novas versões.

↳ Alguns aspetos relacionados com a segurança da informação:

- Garantia do funcionamento do *software*;
- Apoio técnico gratuito (durante um tempo limitado);
- Acesso a formação, seminários e documentação;
- Inexistência de "vírus informáticos".

7. FORMAÇÃO DOS UTILIZADORES

Muitos dos danos na informação ocorrem devido a falta de conhecimentos sobre:

- O *software* utilizado;
- O que fazer como medidas preventivas de segurança de informação.

↳ **Definir um conjunto de procedimentos de trabalho para os vários utilizadores**.

↳ **Desenvolver planos de formação adequados ao *software* utilizado**.

- Para conhecer os programas e como utilizá-los;
- Para evitar erros de utilização devido ao uso de "funções desconhecidas" e à autoformação.

8. UNIDADES DE ALIMENTAÇÃO ININTERRUPTA

9. SEGUROS PARA EQUIPAMENTO ELETRÓNICO

A maior parte dos seguros multirriscos que abrangem o roubo de equipamentos, incêndios, inundações não protegem contra descargas elétricas e oscilações de tensão.

↳ A destruição da informação e equipamentos na sequência de um destes fenómenos não são normalmente incluídos, requerendo um pedido específico do cliente.

SEGURANÇA DOS SISTEMAS DE INFORMAÇÃO – PARTE III

1. ENCRIPTAÇÃO E AUTENTICAÇÃO

São fundamentais na garantia de diversos aspetos da **segurança** das **comunicações** e do **acesso a recursos**.

- Confidencialidade;
- Integridade;
- Não repúdio;
- Controlo de acesso.

Utilização de chaves (públicas ou privadas) para codificação e descodificação.

2. ENCRIPTAÇÃO

A transmissão de dados confidenciais ou sensíveis deve usar a encriptação.

↳ Objetivos:

- Salvaguardar a informação de pessoas que não o destinatário;
- O processo de encriptação deverá ser relativamente rápido de efetuar;
- O processo inverso, executado por não destinatários, deverá ser extremamente difícil de conseguir.

3. CRIPTOGRAFIA

Estudo dos mecanismos de encriptação e desencriptação de informação.

↳ Utilização de um ou mais algoritmos para codificação/descodificação e uma ou mais chaves.

↳ As exigências de conferir confiabilidade e privacidade às informações veiculados na Internet tem incentivado matemáticos e engenheiros a procurar soluções capazes de tornar o uso da rede mundial de computadores numa operação mais segura.

4. CRIPTOGRAFIA – ANALOGIA ENCRIPTAÇÃO/COFRE-FORTE

5. CRIPTOGRAFIA – TERMINOLOGIA

Criptografia	o Arte de escrever de forma escondida; o Serve para garantir a privacidade da informação;
Criptanálise	o Arte de violar sistemas criptográficos ou informação criptografada.
Criptologia	o Criptografia + criptanálise.

Cifra:

↳ Técnica concreta de criptografia.

6. ALGORITMOS DE TRANSPOSIÇÃO

Método criptográfico hebreu	o **Era chamado de *atbash;*** o **Invertia-se o alfabeto;** o **Cada letra do alfabeto original era mapeada numa letra do alfabeto invertido.**
Método romano	o Criaram um tipo de cifra similar à cifra *atbash*; o Em vez de uma inversão, aplicava-se um deslocamento de 3 letras no alfabeto.

7. ENCRIPTAÇÃO – ALGORITMOS

Algoritmos utilizando chaves	Algoritmos sem utilização de chaves
o **O valor da encriptação não está no algoritmo utilizado mas sim na <u>chave</u> utilizada.**	o *One-way transformation*; o Conhecidos como algoritmos *Hash*; o Não utilizam chaves.

8. ENCRIPTAÇÃO SIMÉTRICA

Encriptação com chave secreta (*Secret Key Encryption*).

↳ É usada a mesma chave na codificação e descodificação da informação.

↳ Se apenas o emissor e recetor conhecerem a chave, apenas estes têm acesso ao conteúdo da mensagem.

↳ <u>Problemas</u>:

- Gestão das chaves secretas na geração e distribuição: manutenção do secretismo das chaves.

↳ Vantagens:

- Pode ser implementado em *hardware*;
- Por isso é muito utilizado para garantia da confidencialidade.

Algoritmos

- Operam sobre blocos de informação de tamanho;
- A mensagem é previamente dividida em blocos que são depois combinados e codificados;
- Vários modos de partição, combinação e codificação.
- Algoritmos mais comuns: DES; IDEA.

9. ENCRIPTAÇÃO ASSIMÉTRICA

Encriptação com chaves (*Public Key Encryption*).

↳ São usadas 2 chaves:

- Privada ou secreta;
- Pública ou não secreta.

↳ Permitem (dependendo da sequência de uso):

- Confidencialidade/integridade;
- Não repúdio/autenticação.

Processo 1

Baseia-se na geração de um par de chaves – chave privada e correspondente chave pública – para cada utilizador com que se quer comunicar.

↳ Chaves públicas trocadas livremente: qualquer mensagem codificada usando uma dada chave pública só pode ser descodificada com a respetiva chave privada e vice-versa.

Processo 2

Se utilizador A quiser enviar uma mensagem ao utilizador B com garantia de autenticidade:

- Utilizador A codifica a mensagem a enviar com a sua chave privada;
- Envia a mensagem codificada.

↳ O utilizador B pode descodifica-la com a chave pública do utilizador A;

↳ Como só o utilizador A tem a sua chave privada, só ele poderia ter enviado a mensagem.

↳ Desvantagens:

- Qualquer utilizador com acesso à chave pública do utilizador A poderá descodificar a mensagem;
- Não e garantida a confidencialidade.

A confidencialidade e a autenticidade poderão ser garantidas em simultâneo se a mensagem for encriptada 2 vezes.

- 1ª com chave pública de B;
- 2ª com chave privada de A.

Tipos de segurança assegurados

Chaves usadas na codificação	Chaves usadas na descodificação	Tipos de segurança conseguidos
Pub B	Pri B	Integridade; Confidencialidade
Pri A	Pub A	Autenticação; Não Repúdio
Pub B + Pri A	Pub A + Pri B	TODAS

10. ASSINATURAS DIGITAIS

Objetivo	Método
o Atestas identidade do remetente; o Atestar integridade da mensagem/documento.	o Combinação de: encriptação assimétrica; funções de *Hashing*.

Função *Hashing*

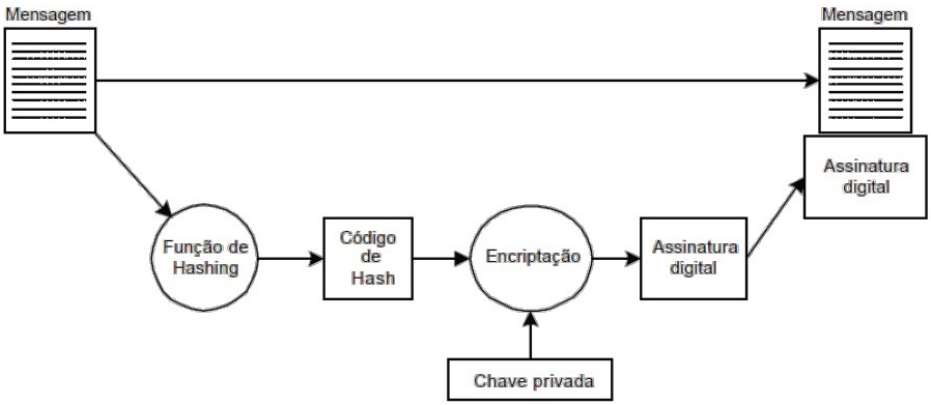
Gera um código de tamanho fixo – código de *Hash* – a partir de uma mensagem ou documento de qualquer tamanho.

↳ Uma mesma mensagem produz sempre o mesmo código de *Hash*.

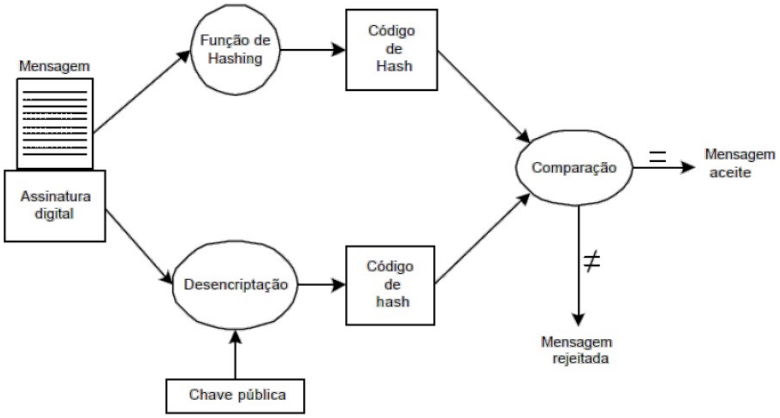
↳ A probabilidade de duas mensagens gerarem o mesmo código de *Hash* é muitíssimo pequena.

↳ As funções de *Hash* são unidirecionais: a partir deste código é, na prática, impossível de obter a informação adicional.

Envio de mensagem digitalmente assinada



Receção de mensagem digitalmente assinada



11. AUTENTICAÇÃO

Mensagem assinada digitalmente contendo a chave pública de um dado utilizador ou entidade.

↳ A assinatura digital garante integridade e autenticidade da chave pública.

↳ Os certificados digitais são gerados por uma entidade de certificação e obedecem à recomendação X.509 da ITU-T.

12. OBTENÇÃO DE CHAVE PÚBLICA

Utilizador A pretende a chave pública do utilizador B.