Segurança da Informação e proteção de dados

Luis Borges Gouveia
Professor Catedrático
lmbg@ufp.edu.pt
http://homepage.ufp.pt/lmbg
Universidade Fernando Pessoa
V3.7, Março de 2017

Âmbito e objetivos destes slides

- Coleção de slides para suporte de introdução ao tema da segurança da informação e da proteção de dados
- Objetivos
  - Sensibilizar sobre a necessidade de desenvolver uma cultura de segurança
  - Alertar para as vulnerabilidades e necessidades de pensamento de segurança para indivíduos e empresas, na nossa sociedade
  - Introduzir conceitos e problemáticas associadas com os temas em questão
  - Enquadrar práticas, lei(s) e instituições relevantes no contexto nacional e internacional
  - Proporcionar uma estrutura (de organização do tema) para o posterior aprofundamento do tema

O contexto atual, a tecnologia, as pessoas e a sociedade

SOCIEDADE DA INFORMAÇÃO

Luís Borges Gouveia, lmbg@ufp.edu.pt

tecnologia

- *minimização de esforço*, conceito de utilidade para o indivíduo

  Ortega Y Gasset

- algo que as pessoas criam para usar e alterar o seu estilo de vida ou o ambiente circundante
  - http://www.links.net/vita/swat/course/thesis/tech/

Luís Borges Gouveia, lmbg@ufp.edu.pt

As modificações da tecnologia

A **ciência** descobre
A **indústria** aplica
O **homem** adapta-se

Mote da Feira Mundial de Chicago, 1933

As **pessoas** propõem
A **ciência** estuda
A **tecnologia** adapta

Mote centrado nas pessoas para o Séc. XXI

Donald Norman, *Things that made us smart*, 1993. Addison Wesley

Tecnologias de Informação

Definição:

- Termo que engloba todas as formas de tecnologia para criar, armazenar, trocar e utilizar informação de várias origens (análógico, digital ou dados de atividade comercial, conversações em voz, imagens, filmes, apresentações multimedia) e outras formas, incluindo aquelas que ainda não foram concebidas
- Inclui as comunicações e os computadores num mesmo contexto
- Referida como o tipo de tecnologia que suporta a revolução da informação ou a era da informação

Vários termos:

- Tecnologias de Informação (TI)
- *Novas* Tecnologias de Informação (NTI)
- Tecnologias de Informação e Comunicação (TIC)
- Tecnologias de Informação *Emergentes* (TIE)
- Telecomunicações, Media e Tecnologias (TMT)

TIs – Leis de Murphy

- "*se existem duas ou mais alternativas para fazer a mesma coisa, e uma dessas alternativas pode resultar em catástrofe, então alguém a escolherá*"

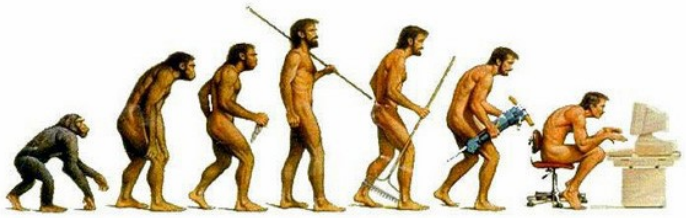
  Edward Murphy, engenheiro da USAF, 1947

- Conjunto de princípios que oferecem uma abordagem irónica, mas que a experiência mostra, por vezes, poderem acontecer.
- Alguns exemplos:
  - Um dispositivo falha no momento menos oportuno
  - Um objeto cai de modo a causar o máximo de prejuízo em si ou noutros objetos
  - A tendência de um objeto para cair é diretamente proporcional ao seu valor
  - Se um dispositivo pode vir a funcionar mal, tal acontecerá
- Lei de dinâmicas negativas de Finagle
  "*se alguma coisa pode correr mal, então correrá mal (e na pior altura possível)*"

  Larry Niven, escritor de ficção científica

Dimensões do uso das TIC

- Individual
- Grupo de indivíduos
- Comunidade
- Sociedade



Individual

- único, separado
- "de ou sobre" uma pessoa
- caraterística de uma só pessoa
- referência a determinado ser humano
- uma pessoa de um determinado tipo

- qualquer um de nós pode ser referido como um indivíduo e constitui um seu representante
- Por vezes também usado o termo pessoa ou, no contexto da informática (e por complemento ao uso de unidades digitais), por unidade de carbono

Grupo

- um determinado número de pessoas associadas ou atuando em conjunto
- possui um conjunto de regras bem definidas, a maior parte das vezes formais e pré estabelecidas
- reunir ou formar um grupo, com objetivos, regras, constituído por várias pessoas
- associado ao conceito de conjunto, em que um grupo pode ter zero, um ou mais elementos
  - as empresas podem ser vistas como um bom exemplo de um grupo de individuos, associado com regras formais e (espera-se) bem definidas

Comunidade

- pessoas que vivem num dado lugar, região ou país, considerado como um todo
- grupo de pessoas com a mesma religião, raça, ocupação, etc.
  - interesses, que definem o valor
  - condição de partilha, com aspetos em comum ou possuir semelhanças de qualquer tipo
  - Também pode referir um grupo de animais ou plantas vivendo no mesmo lugar (não relevante no presente contexto)
  - as regras são essencialmente informais e resultado da evolução da própria comunidade (ou, no mínimo, aceites sem contrapartidas de contratos ou meios mais formais)

Comunidade virtual

- comunidade de pessoas partilhando os mesmos interesses, ideias ou sentimentos através da Internet ou outras redes de colaboração (normalmente plataformas digitais)
  - agregações sociais que emergem da Internet quando um número suficiente de pessoas se envolvem em discussões públicas por um período de tempo alargado, com empenho humano, que permita a criação de redes de relacionamentos pessoais no ciberespaço (Howard Rheingold)
  - as comunidades virtuais podem ser vistas como subgrupos de acordo com a noção de ciberpespaço de aldeia global (Marshall McLuhan)

O que são comunidades virtuais

- organizadas em torno de afinidades, interesses partilhados, reunindo pessoas que não necessitam de se conhecer antes de se encontrarem em linha
  - meios do tipo muitos para muitos (N:M): ao contrário de poucos para muitos (n-M) – difusão ou de um para um (1:1) – telefone e SMS, permitem que grupos de pessoas comuniquem com muitos outros grupos de pessoas
  - qualquer dispositivo de TIC tornou-se um meio de publicação impressa, uma estação de difusão e um local de encontro
  - sistemas baseados em texto evoluiram para suportar comunicações multimédia e permitem o uso contínuo de voz e imagem
  - relativamente dissociadas da vida social face a face que caraterizam as comunidades de proximidade geográfica
  - pessoas que comunicam globalmente, não vivem suficientemente perto para se encontrarem face a face regularmente

Comunicações móveis

- organizadas em torno de redes sociais. As pessoas ligam e enviam mensagens essencialmente para quem já conhecem
  - comunica-se mais com quem já está na nossa agenda
  - acessível em qualquer lugar, a qualquer hora e sempre disponível.
  - a Internet está agora disponível como de uma nuvem de dados sempre presente e disponível
  - emergem crescentes capacidades de comunicação multimédia
  - toques personalizados e imagens engraçadas são o início, as aplicações tornam-se mais sofisticadas e incluem video a tempo real, as aplicações colaborativas e de realidade aumentada, quer em jogos, quer em contexto profissional
- intimamente relacionado com o comportamento das pessoas no espaço físico. Tem forte influência na forma como pequenos grupos coordenam as suas atividades numa comunidade baseada na proximidade geográfica

Comunicações virtuais móveis

- sistemas muitos para muitos (N:M), sempre disponíveis
  - comunidades virtuais e de recursos da Internet acessíveis instantâneamente para as pessoas e para os seus agentes (software), independentemente de onde se encontrem (local de trabalho, em trânsito, em casa ou em viagem)
  - usados para coordenar de grupos no espaço geográfico, desde a socialização até actividade de mobilização política
  - ambientes de jogos, arenas sociais, media artísticos, ferramentas de negócios, armas políticas
- como qualquer outro media associado com as comunidades virtuais, inicia-se com os jovens como meio de lazer e interação social e difunde-se a outras instituições

Luís Borges Gouveia, lmbg@ufp.edu.pt

Sociedade

- sistema complexo em que as pessoas vivem em conjunto, em comunidades organizadas
  - pessoas no geral, em contexto de interação livre
  - uma comunidade de pessoas que vivem num país ou região e possuem costumes, leis e organizações comuns
  - uma organização de pessoas, formada com um determinado fim (clube ou associação)
  - classe de pessoas que determinam a moda, ricas, influentes e constituem a classe dirigente de um local (alta sociedade)
  - a situação de estar com outras pessoas

Luís Borges Gouveia, lmbg@ufp.edu.pt

Sociedade da informação (e do conhecimento)

- define uma sociedade em que a distribuição e a manipulação de informação se torna a mais significativa e importante atividade económica e cultural
- distingue-se de sociedades que predominantemente se afirmam como industriais ou agriculas e dessa forma, constitui uma Terceira vaz civilizacional (conceito de terceira vaga, introduzido por Alvin Tofler)
- as máquinas da sociedade de informação são os computadores e as telecomunicações, igualmente elementos importantes das designadas tecnologias de informação e comunicação

Luís Borges Gouveia, lmbg@ufp.edu.pt

Declaração política do G8

- "*As TIC estão a mudar a forma como vivemos: como trabalhamos e fazemos negócios, como educamos as nossas crianças, estudamos e investigamos, nos treinamos a nós mesmos e como nos divertimos*
- *A sociedade da informação não afeta apenas o modo como as pessoas interagem, mas requer também das organizações tradicionais que sejam mais flexíveis, mais participativas e descentralizadas*"

Conferência de Ministros sobre a Sociedade da Informação, Fevereiro de 1995

Luís Borges Gouveia, lmbg@ufp.edu.pt

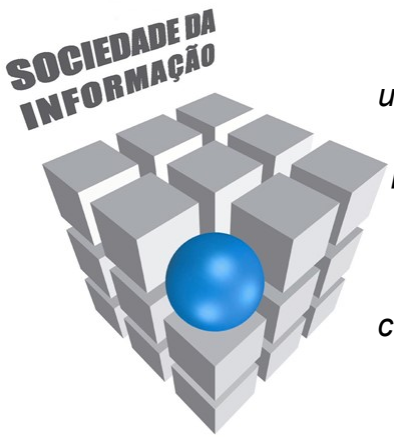
Uma definição de sociedade de informação

- "*a society characterised by a high level of information intensity in the everyday life of most citizens, in most organisations and workplaces; by the use of common or compatible technology for a wide range of personal, social, educational and business activities, and by the ability to transmit, receive and exchange digital data rapidly between places irrespective of distance.*"

IBM, 1997

Luís Borges Gouveia, lmbg@ufp.edu.pt

A sociedade da informação



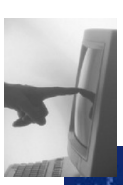
A Sociedade da Informação é uma sociedade que predominantemente utiliza as tecnologias de informação e comunicação para a troca de dados e informação em formato digital e que suporta a interação entre indivíduos e organizações com recurso a práticas e métodos em construção permanente

(Gouveia e Gaio, 2004)

Luís Borges Gouveia, lmbg@ufp.edu.pt

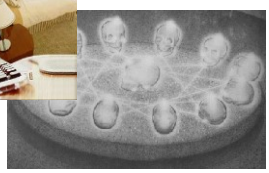
Sociedade da informação
3 caraterísticas essenciais

Uso intensivo de tecnologias de informação e comunicação



Uso crescente do digital

Organização em rede



Luís Borges Gouveia, lmbg@ufp.edu.pt

A sociedade da informação (I)

Dados de 1997…

- um gestor que trabalha em média 30 h, usa mais de 1 milhão de folhas de papel (3,8 ton de papel)
- só nos EUA são processados por dia mais de 35 mil milhões de documentos em papel
- geram-se 75 mil milhões de novas informações anualmente
- o gestor lida atualmente com um excesso de informação - *infoglut*

...e excesso de informação causa stresse!

Luís Borges Gouveia, lmbg@ufp.edu.pt

A sociedade da informação (II)

- A passagem da sociedade industrial para a sociedade de informação já ocorreu nos EUA em 1950! (tendo por base, o número de empregos…)
  - o número de empregos em informação ultrapassou no final do século XX, a soma dos empregos nos setores de agricultura, industria e serviços
- A sociedade moderna é orientada pela tecnologia, com constantes mudanças das suas caraterísticas (e numa taxa cada vez mais acelerada)

Luís Borges Gouveia, lmbg@ufp.edu.pt

Desenvolvimento no sector da informação (I)

- Aumento da literacia de computadores
  - dos líderes e da população em geral
- Crescente importância das telecomunicações
  - dos satélites às redes e as bases de dados internacionais
- Desenvolvimento dos computadores pessoais
  - transformação, vulgarização e proliferação
  - evolução para dispositivos móveis
  - aparecimento massivo de objetos inteligentes
- Interligação de equipamentos de processamento de dados
  - computadores domésticos e empresariais, interligados entre si e com acesso a bases de dados
  - sensores e atuadores
  - a computação em núvem (*cloud*)
  - a Internet das Coisas (IoT)

Luís Borges Gouveia, lmbg@ufp.edu.pt

Desenvolvimento no setor da informação (II)

- Computadores como pensadores da parte esquerda do cérebro – "a máquina analítica"
  - crescente importância da inteligência artificial (e de agentes autónomos)
  - inteligência competitive e análise de informação
- Crime informático e segurança informática
  - privacidade e sigilo (proteção de dados pessoais)
  - segurança da informação
- Novos suportes multimédia de informação
  - servindo diferentes industrias, com diferentes interesses
  - industrias criativas e de entretenimento
- Aproximação entre homem e máquina
  - crescente importância dos fatores humanos
- Autonomia, mobilidade e adaptabilidade
  - *anytime, anywhere, anyhow, anything*

Lei da sobrevivência de Murdick

À medida que a informação disponível para os gestores aumenta em quantidade e velocidade, o fluxo de informação deve ser de maior seletividade

sistemas de informação modernos e de maior sofisticação devem proporcionar aos gestores, tanto o acesso à informação ambiente (exterior à organização) como à informação gerada internamente na organização

Esta lei é dos anos 80 do século passado e ainda não tem em conta o uso da informação como arma competitiva e de confrontação, entre diferentes empresas, indivíduos e organizações – o que torna ainda mais premente a importância da informação

Alguns dos pensadores que influenciaram o conceito atual de Sociedade da Informação

- Não existe uma lista que seja consensual
- Não se pretende excluir outros com igual mérito
- Representa um conjunto de ideias de força que moldaram a visão atual da sociedade da informação
  - originaram outros nomes como Bill Gates (Microsoft), o Steve Jobs (Apple), o Mark Zuckerberg (Facebook) ou o Serge Brin e Larry Page (Google)…




O campeão da usabilidade e dos fatores humanos na tecnologia

- *a maior a parte dos problemas que o desenvolvimento de produtos seguros, mais fiáveis e fáceis de usar e entender enfrenta, não são tecnológicos: são sociais e organizacionais*
- *usabilidade e artefatos de informação*

Donald Norman
http://www.jnd.org/

O virtual – Pierre Lévy

o teórico da redefinição das relações humanos com e no espaço e tempo digitais

O digital e o uso intensivo de computadores e redes proporciona uma nova dimensão de interação que é economicamente e socialmente tangível
O virtual redefine as noções de tempo, espaço e a própria noção de conhecimento

http://www.youtube.com/watch?v=_DOSAf_esws

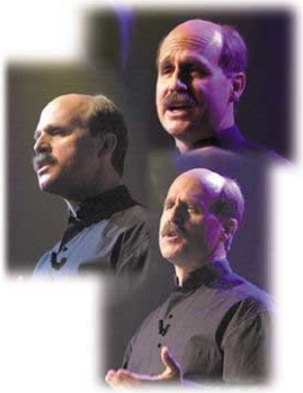
Dos átomos aos bits

Interagir no mundo real é cada vez mais interagir com uma relação de espaço físico e espaço virtual, onde a importância dos átomos cede progressivamente lugar ao mundo dos bits, da informação no digital

o evangelizador do uso das TIC para o dia a dia, popularizando o digital como primeira opção para lidar com a informação
http://web.media.mit.edu/~nicholas/

Paul Saffo

- *"the S curve*
  Most technologies take 20 years to become an overnight success (the bottom of the S), which is a long line running horizontally until, 20 years later, it takes off, suddenly rising vertically: the "riser" part of the letter. Then the top "cap" of the "S" takes over with a straight line, and the letter is complete."
- *no que respeita à Internet, estamos ainda na sua infância – todas as ocorrências que estamos a viver são ainda o seu início*
- *estamos à deriva num mar de informação, que temos de navegar com ferramentas que estão longe de serem as adequadas*
- *http://www.saffo.com/*
- *Institute for the future: http://www.iftf.org*



Al Gore

Al Gore foi um dos primeiros defensores da existência de uma infra-estrutura de comunicação de dados de alta velocidade, e que entendeu bem cedo como esta visão poderia levar ao incremento do desenvolvimento económico e social dos Estados Unidos

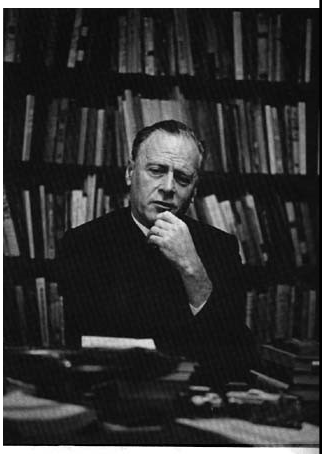
Discurso 1994...

http://www.ibiblio.org/icky/speech2.html

"We shape our tools and thereafter they shape us"

"...if you accelerate any structure beyond a certain speed it collapses"

- ideólogo da revolução da informação, contribuiu para o conhecimento actual dos modos mentais, gráficos, mapas e meios de aprendizagem prática que são correntes na nossa sociedade para lidar com o que ele próprio designou ser a idade da informação
- http://www.marshallmcluhan.com/



Marshall McLuhan in the early 1970s.
(Photo: Horst Ehricht)

"*Societies have always been shaped more by the nature of the media with which people communicate than by the content of the communication*"

Conhecido pelas suas visões originais sobre os media, McLuhan introduziu os conceitos associados às frases: "***o meio é a mensagem***" e "**aldeia global**"

- *no livro "The Skin of Culture" sugere que a súbita modificação sem preparação e o aumento de ritmo de mudança, pode levar à desintegração e quebras do sistema*
- *um dos problemas dos meios eletrónicos (em especial com as redes) é ser quase impossível esconder qualquer coisa. Algo que seja secreto ou esteja escondido tende a ser aberto*
- *a enfatização de um ambiente electrónico amplifica a emoção em vez da resposta racional*
- *quando a informação se move a uma velocidade eletrónica, os mundos das tendências e dos rumores transformam-se no mundo real*

Derrick de Kerckhove
http://www.mcluhan.utoronto.ca/derrickdekerckhove.htm

Manuel Castells

- *o último quarto do séc. XX viveu uma revolução tecnológica que transformou o nosso modo de pensar, de produzir, de consumir, de vender, de questionar, de comunicar, de viver e morrer*
- *todas estas modificações geraram grandes mudanças na produtividade, …*
- *este panorama significa um incremento da desigualdade social que exclui do sistema as pessoas, grupos e regiões sem capacidade de gerar valor como produtores ou consumidores*

A Sociedade em rede

http://www.indiana.edu/~tisj/readers/full-text/14-4%20Stalder.html

http://globetrotter.berkeley.edu/people/Castells/castells-con0.html

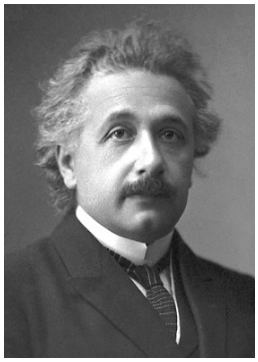
Prever e perspetivar tecnologia

TECNOLOGIAS E CONTEXTOS

Luís Borges Gouveia, lmbg@ufp.edu.pt

"A man should look for what is, and not for what he thinks should be"

Albert Einstein
(1879-1955)



O canivete Suiço

Canivete é um utensílio multi-uso moderno que compreende um agrupamento de elementos da cutelaria e outros mais ou menos usuais de fácil portabilidade.
Fonte: *pt.wikipedia.org*

indústria

Fazer produtos

Fatores de produção

Trabalho especializado

Fatores de escala

Novos mercados e concorrência

Feiras industriais

Design

Luís Borges Gouveia, lmbg@ufp.edu.pt

O canivete Russo

Luís Borges Gouveia, lmbg@ufp.edu.pt

soberania

Capacidade e logística

Diplomacia e poder

Assegurar inteligência

Fazer alianças

Defender interesses

Sustentabilidade económica e social

Ideologia, bandeira e nação

Luís Borges Gouveia, lmbg@ufp.edu.pt

O canivete digital

Luís Borges Gouveia, lmbg@ufp.edu.pt

convergência

Representação da informação

Persistência e preservação de dados

Memória e organização

Multimédia, serviços e aplicações

Computadores e redes

Inovação e criatividade

Tempo e espaço digital

Luís Borges Gouveia, lmbg@ufp.edu.pt

O canivete comunicação

Luís Borges Gouveia, lmbg@ufp.edu.pt

proximidade

Logística e estar perto

Mobilidade

Espaço, tempo e ubiquidade

Serviços de localização

Autonomia e independência

Disponibilidade e acesso

Redes sociais e temáticas

Luís Borges Gouveia, lmbg@ufp.edu.pt

O canivete do futuro

Luís Borges Gouveia, lmbg@ufp.edu.pt

adaptação

Desmaterialização da informação

Funcionalidade e serviços

Modelos de negócio mutantes

Aprendizagem contínua

Redes emergentes

Serviços de contexto e conhecimento

Interação e relacionamento

Luís Borges Gouveia, lmbg@ufp.edu.pt

"You can never plan the future by the past"

Edmund Burke

(1729-1797)

Luís Borges Gouveia, lmbg@ufp.edu.pt

um exercício simples

– era uma vez, em três passos –

telemóveis
cartões de débito/crédito

Luís Borges Gouveia, lmbg@ufp.edu.pt

Testar a dependência

1

- Passar 10 dias **sem** estes dois objetos…

Luís Borges Gouveia, lmbg@ufp.edu.pt

Potencial e utilidade

- Descrever 10 dias **com** estes objetos

Luís Borges Gouveia, lmbg@ufp.edu.pt

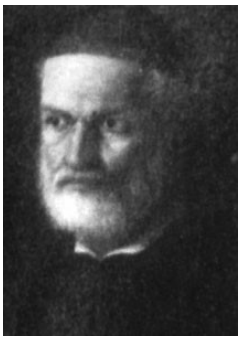
Prever futuro sem os seus artefatos

- Descrever 10 dias de **hoje**, 10/20 anos **atrás**

Luís Borges Gouveia, lmbg@ufp.edu.pt

"Nós somos o que fazemos. O que não se faz não existe. Portanto, só existimos quando fazemos. Nos dias que não fazemos, apenas duramos"

Padre
António Vieira
(1608-1697)



Resumindo, da Sociedade da Informação ao uso e exploração do digital

CONTEXTO

A ideia de mundo

Agora…

Sociedade da Informação

- Uso intensivo de computadores e redes
  (*do saber usar ao **saber o que fazer com eles***…)
- A informação que conta é digital
  (*a informação já **não é o que era e vale pouco***…)
- A organização que conta é a rede
  (*as hierarquias são uma **simplificação no momento***…)

O que significa?

Mudança…

Luís Borges Gouveia, lmbg@ufp.edu.pt

Sobre o conceito de mudança

- ***"...quando um príncipe deixa tudo por conta da sorte, ele se arruína logo que ela muda. Feliz é o príncipe que ajusta seu modo de proceder aos tempos, e é infeliz aquele cujo proceder não se ajusta aos tempos."***
- ***"Uma mudança deixa sempre patamares para uma nova mudança."***

Nicolau Maquiavel (1469, 1527)

Luís Borges Gouveia, lmbg@ufp.edu.pt

Dois aspectos essenciais

- **Sustentabilidade**

Como garanto a minha liberdade ou como o valor gerado cobre o valor absorvido*
**(valor: económico, social, político e satisfação)*

- **Soberania**

*Como garanto a minha identidade** ou como posso ser reconhecido como eu próprio e ser o que quero/posso ser*
***(marca: pessoa, empresa, nação)*

Luís Borges Gouveia, lmbg@ufp.edu.pt

Tempo e espaço

- **Tempo**

  24/7 sempre ligado, sempre presente

  MAS exige disponibilidade inteligente e bem gerida

  AFINAL o tempo humano é limitado

- **Espaço**

  em qualquer lugar, de qualquer forma

  MAS como estar presente?

  AFINAL a experiência é o memorável

Luís Borges Gouveia, lmbg@ufp.edu.pt

Estratégias facilitadas pelo digital

- Capacidade de **projeção**
  - Chegar aos outros e exposição global
- Diferente e **dinâmico**
  - Ter capacidade de capturar a atenção
- **Criativo** e **inovador**
  - Ter capacidade de concretizar valor
- **Inclusivo** e **cumplice**
  - Perceber que a colaboração e a rede são essenciais

Contexto

- Mundo complexo
  - Computadores e redes (tudo ligado)
  - Mais gente com competências à escala gobal
- Exigidos novos cuidados ou o reforço dos existentes
  - …e alargado a mais pessoas e empresas
  - As instituições são alvo
  - As figuras públicas são alvo
  - No geral, quem pode contribuir (*) é alvo

Terminologia base para iniciar a discussão do tema

CONCEITOS PARA O ESTUDO DA SEGURANÇA DA INFORMAÇÃO

Luís Borges Gouveia, lmbg@ufp.edu.pt

Segurança...

- Um ativo central e não muitas vezes valorizado
  - Não existindo, sentimos muito a sua falta
  - Existindo, *continuamos como estamos…*
- Não tem retorno direto e funciona para um potencial risco que esperemos que não ocorra
  - Tal como um seguro (em que o risco é normalmente público – acidente. Em oposto a ser privado – incidente)
- Segurança e defesa
  - Conceito associado com muitas outras atividades e que determina a nossa qualidade de vida e nível de proteção
  - Ativo não tangível que afeta confiança (a moeda de esperança da economia…)

Luís Borges Gouveia, lmbg@ufp.edu.pt

Informação...

- Apoia a tomada de decisão e torna possível a ação
  - É abstrato, mas central à atividade humana
- Pode ser um **recurso**
  - E portanto estratégico numa organização (por exemplo, informação comercial de clientes e fornecedores…)
- Pode ser um **ativo**
  - E pode ser transacionado (por exemplo, vender uma base de dados de clientes e suas caraterísticas…)
- Pode ser uma ***commodity***
  - Adquiriu um valor de mercado expetável (por exemplo, saber onde fica determinado lugar…)

Informática...

- Lidar com a informação digital
  - Processada, armazenada e comunicada por dispositivos eletrónicos
- Muito além do computador
  - Dispositivos móveis: *tablets*, *smart phones*, …
  - Sistemas de geolocalização e identificação e controlo de acessos, …
  - Armazenamento de dados: USBs, discos, …
  - Cartões e outros meios de identificação
  - Internet, *Cloud* e plataformas digitais
  - Aplicações , serviços e jogos

Segurança informática

- Vírus e outras formas de ataque a computadores e dispositivos móveis
- Exploração de falhas de software, cada vez mais complexo
- Engenharia social e exploração das caraterísticas humanas (curiosidade, medo, ganância, etc.)
- Falha humana não intencional (desconhecimento, relaxamento ou desinteresse)
- Falha humana intencional (interesses e atividade criminosa)

Segurança da Informação

- Um maior nível de preocupação que inclui a informação digital, mas também a existente em suportes não digitais
- Preocupa-se com uma abordagem estruturada ao problema e à salvaguarda da informação
  - Qual é a informação crítica?
  - Quais as infraestruturas críticas?
  - O que fazer para assegurar a continuidade do negócio/atividade?
- E temos ainda de lidar com a questão final:
  - *Quem guarda os guardas?*

Quis custodiet ipsos custodes?

Um dilema proposto por Juvenal, poeta Romano (quem guarda os guardas?)

Problema inicialmente colocado por Platão (A República, obra sobre governo e moralidade). A sociedade perfeita descrita por Sócrates (personagem principal da obra) depende de trabalhadores, escravos e comerciantes. A classe guardiã protege a cidade. A pergunta é feita a Sócrates, "Quem guardará os guardiões?" ou, "Quem irá nos proteger dos protetores?" a resposta de Platão para esta pergunta é que os guardiões irão proteger-se deles mesmos. Segundo Platão, deve ser contada a eles uma "mentira carinhosa." A mentira carinhosa lhes dirá que os guardiões são melhores do que os que eles servem e é então, responsabilidades deles guardar e proteger aqueles que são menos do que eles. É assim instigado neles um desgosto por poder ou privilégio; eles irão mandar porque eles o acham ser correto, não porque o desejam.

Luís Borges Gouveia, lmbg@ufp.edu.pt

Princípios

- Integridade
  - A informação deve ser completa, verificável e verdadeira
- Confidencialidade
  - A informação deve ser salvaguardada de quem não teve autorização para o seu acesso
- Disponibilidade
  - A informação deve ser fácil de obter onde e quando necessária e de forma entendível
- Não repudiação
  - Não deve ser possível a negação de autoria ou origem da informação

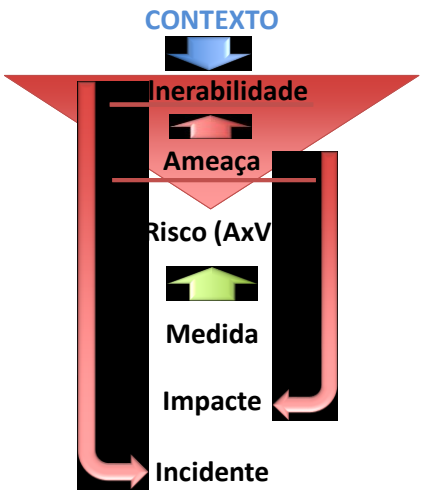
Luís Borges Gouveia, lmbg@ufp.edu.pt

Termos associados: segurança da informação

- Vulnerabilidade
  - Existência de um potencial de falha de segurança
- Ameaça
  - Elementos concretos, potenciadores de exploração de falha de segurança
- Risco
  - Probabilidade efetiva de concretização de ameaças para as vulnerabilidades existentes
- Medida
  - Meio ou procedimento de combate ou minimização do risco
- Impacte
  - Prejuízo em caso de concretização da ameaça
- Incidente
  - Situação efetiva de aproveitamento de uma vulnerabilidade

Luís Borges Gouveia, lmbg@ufp.edu.pt

Termos associados: segurança da informação



Luís Borges Gouveia, lmbg@ufp.edu.pt

O digital versus o humano…

https://techsert.com/why-is-cyber-security-important/

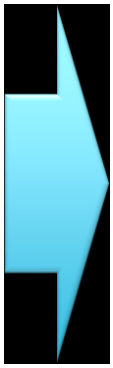
Enquadramento das práticas da segurança da informação num contexto mais global

DESAFIOS DA SEGURANÇA DA INFORMAÇÃO

Conflitos na era da informação

Informação em contexto de guerra

- Inteligência
- Vigilância
- Reconhecimento
- Clima
- Geográfico
- Outro



Guerra da Informação

- Influenciar atitudes
- Negar/Proteger
- Enganar/Esconder
- Explorar/Atacar

Luís Borges Gouveia, lmbg@ufp.edu.pt

Potenciais vulnerabilidades da sociedade

- **Vulnerabilidades das democracias:**
  - tirando partido de liberdades e garantias e originando informação falsa ou confusa em campanhas organizadas com recurso aos media (imprensa, de massas e redes sociais);
- **Ataque de indivíduos criativos**:
  - com conhecimento, capacidade e determinação para explorar sistemas de comunicações e redes de computadores para ganhos ilegais ou simplesmente sabotar a sociedade;
- **Organizações criminosas:**
  - terroristas, traficantes de armas, ou de mão de obra escrava ou orgãos humanos, que operam entre países;
- **Operações conjuntas:**
  - realizadas de forma combinada com ações militares mais tradicionais, ocultando interesses e atacando alvos considerados críticos para esses interesses;
- **Guerra psicológica:**
  - operações com foco na população de modo a minar a sua confiança nos seus lideres ou na sabedoria da suas ações, muitas vezes explorando clivagens étnicas, sociais, morais dessa sociedade

http://www.iwar.org.uk/iwar/resources/deterrence/iwdAppb.htm

Luís Borges Gouveia, lmbg@ufp.edu.pt

Atores principais na guerra da informação

- **Nações mais poderosas**
  - depende de sistemas complexos, sujeitos a instabilidade política ou equilíbrios frágeis e possível perda de reputação
- **Organizações multinacionais e redes muito estruturadas**
  - Sujeitos a ações legais, roubo de propriedade intelectual, falha de sistemas e censura pública
- **Indivíduos e redes menos estruturadas**
  - Sujeitos a stresse legal e ilegal por governos e organizações, quando apanhados

Luís Borges Gouveia, lmbg@ufp.edu.pt

O ciberpoder: 3 táticas (*familiares?...*)

- **AA diz a BB o que fazer**
  - se não, BB não o pode fazer…
- **AA não permite a escolha a BB**
  - inclui AA permitir a BB, aplicar as suas estratégias
- **AA molda as preferências de BB**
  - desta forma, BB não considera algumas das estratégias alternativas, como possíveis

Luís Borges Gouveia, lmbg@ufp.edu.pt

Ciberdefesa

- Conceito militar de resposta à guerra da informação
- Possui 3 componentes:
  - Ciberdefesa **defensiva**: orientada para assegurar a defesa de infraestruturas críticas
  - Ciberdefesa de **exploração**: orientada para explorar e conhecer vulnerabilidade de terceiros e próprias
  - Ciberdefesa **ofensiva**: orientada para realização de ataques a alvos específicos ou como meio de dissuasão (pode incluir o desenvolvimento de ciberarmas)

Luís Borges Gouveia, lmbg@ufp.edu.pt

Cibersegurança

- A versão civil da ciberdefesa, orientada para as preocupações de proteger a sociedade nas suas vertentes de serviços públicos, economia e indivíduos
  - Existem ao nível dos Estados, preocupações crescentes com estas questões (em Portugal, é a ***estratégia nacional para a cibersegurança***, http://www.gns.gov.pt/new-cyberseguranca.aspx da responsabilidade do Gabinete Nacional de Segurança)
  - É organizada em rede e conta com a troca de informação entre interessados e com o reporte de incidentes e práticas de contingência comuns (em Portugal, o **CERT.PT** http://www.cert.pt/)
  - Cada um de nós, deve tomar precauções à sua escala…

Luís Borges Gouveia, lmbg@ufp.edu.pt

Incidentes (alguns exemplos…)

- **Stuxnet** (o caso do ataque com sucesso no Irão) e ?
  - Utilização de software malicioso como ciberarma
- **Wikileaks** e os EUA
  - Classificar informação e proteger informação, parece um ato impossível
  - Ainda existe confidencialidade possível?
- **Snowden** e a NSA
  - Afinal até eu sou espiado, registado e armazenado nas minhas mais diversas dimensões
  - Ainda existe privacidade?
- A **ciberespionagem económica** no caso da China e dos EUA
  - Dos relatórios Mandiant à acusação de Pensilvania
  - Cibersegurança diferente de ciberdefesa?
    E as relações EUA-China?

Numa escala mais humana…

- Como defender:
  - A esfera empresarial
  - A esfera pessoal
- Desafios:
  - Proteção e segurança da informação
  - Privacidade (proteção de dados)
- Mecanismos
  - Trabalho especializado
  - Formação, cautela e experiência

Como fazer?

- Avaliar os ativos de informação
- Classificar a informação
- Listar as infraestruturas críticas
- Listar as vulnerabilidades, as ameaças e os riscos para o contexto
- Formar e enquadrar os recursos humanos
  - Desde o controle de acessos e creditação, até à sensibilização e efetivação de políticas de segurança
- Realizar uma auditoria de segurança
  - Avaliar os riscos e capacidades existentes, refletindo sobre impactes e medidas de contingência
- Rever, partilhar e colaborar
  - A segurança é partilha de informação, rede e conhecimento…

Luís Borges Gouveia, lmbg@ufp.edu.pt

Porquê estudar o tema?

- A melhor maneira de estar seguro é estar informado
- As proteções tem de ser uma preocupação constante
  - Cada vez mais sofisticadas as ameaças e de maior alcance
  - Sempre em evolução, a exigir uma vigilância contínua
  - Os indivíduos são tão importantes como as empresas
- O conhecimento é a arma e a colaboração a defesa
  - As redes são importantes e as colaborações e parcerias estratégias
  - O nível de segurança corresponde ao nível associado com o nodo mais vulnerável da rede a que pertencemos

Luís Borges Gouveia, lmbg@ufp.edu.pt

1.1. Conceitos associados
1.2. Tipos de dados e classificação da informação
1.3. Avaliação de risco e mecanismos de controlo (de acessos)
1.4. Normalização e práticas correntes
1.5. A perspetiva das organizações
1.6. A perspetiva dos indivíduos

SEGURANÇA DA INFORMAÇÃO

Luís Borges Gouveia, lmbg@ufp.edu.pt

Enquadramento operacional do tema

SEGURANÇA DA INFORMAÇÃO

Luís Borges Gouveia, lmbg@ufp.edu.pt

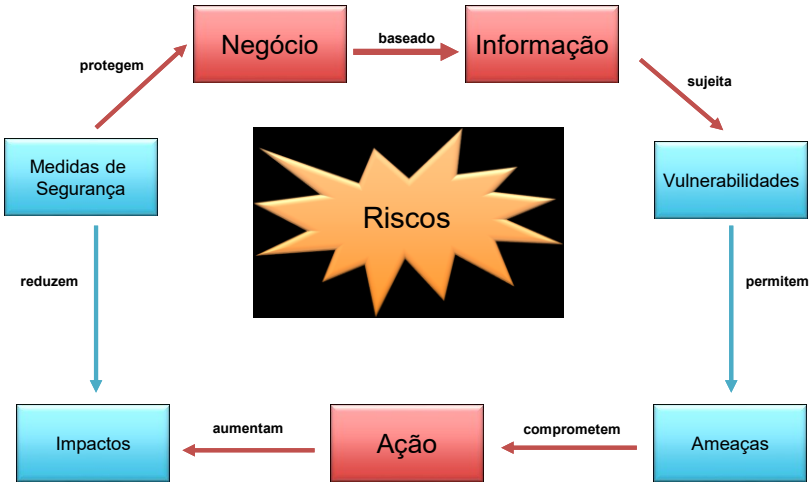
Cenário Actual

- Era da Informação e da Globalização (Sociedade da Informação)
  - Avanços nas tecnologias de informação
  - Avanços nas telecomunicações
  - Maior rapidez na troca de informação
  - Maior exigência das pessoas
- Globalização das ameaças
- Novos riscos e vulnerabilidades

Segurança da Informação

- Proteção da informação e do conhecimento sensíveis para a garantia de continuidade do negócio da empresa
  - *informação* **diferente de** *informações*
- Questões importantes:
  - **O que** deve ser protegido?
  - **Contra o que** será necessário proteger?
  - **Como** será feita a protecção?

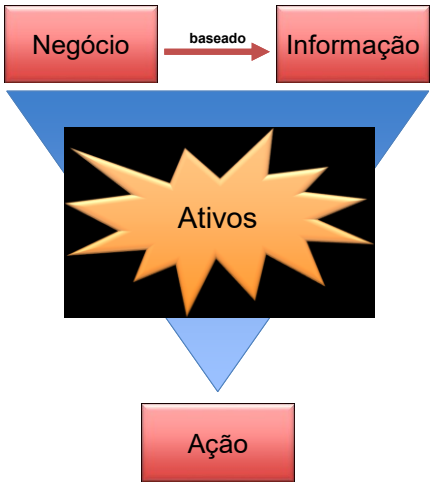
Ciclo da segurança da informação



Luís Borges Gouveia, lmbg@ufp.edu.pt

Ciclo da segurança da informação

Não existe um ambiente 100% seguro, mas um ambiente com menos risco



Luís Borges Gouveia, lmbg@ufp.edu.pt

Principais Ameaças

Tipo	Causas
1. Atos de falha ou erro humano	Acidentes, erros de trabalhadores
2. Comprometimento de propriedade intelectual	Pirataria, ofensas aos direitos de autor
3. Atos deliberados de espionagem ou intrusão	Acessos não autorizados e/ou recolha de dados
4. Atos deliberados de extorsão de informação	Chantagem de divulgação de informação
5. Atos deliberados de sabotagem ou vandalismo	Destruição de sistemas ou informação
6. Atos deliberados de roubo	Tomada ilegal de equipamento ou informação
7. Ataques de software	Vírus, *worms*, macros, negação de serviço
8. Forças da natureza	Fogo, inundações, terramotos, trovoadas
9. Desvios na qualidade de serviço, dos fornecedores de serviço	Rede elétrica e rede de telecomunicações
10. Erros ou falhas técnicas de hardware	Falhas de equipamentos
11. Erros ou falhas técnicas de software	Bugs, problemas de código, erros de conceção
12. Obsolescência tecnológica	Tecnologias ultrapassadas ou obsoletas

Exemplo no setor da Banca (ameaças)

http://www.isdecisions.com/blog/it-infrastructure/information-security-in-banking-insider-threat/

Pessoas são chave!

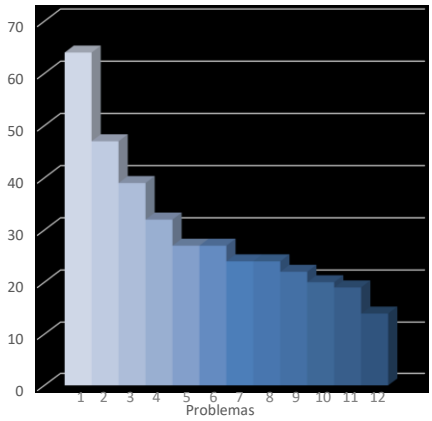
http://opinionator.blogs.nytimes.com/2013/01/13/what-is-a-hacktivist/

Principais obstáculos

Descrição
Falta de consciência dos responsáveis de alta direção
Dificuldade em demonstrar o retorno
Custos de implementação
Falta de consciência dos utilizadores
Falta de prioridade
Falta de recursos financeiros ou de orçamento
Falta de competências ou profissionais capacitados
Falta de ferramentas
Outras, mais específicas do setor de atividade ou do contexto próprio

Principais Problemas Encontrados

Questionário da revista CIO e PricewaterhouseCoopers – 54 países (2009)

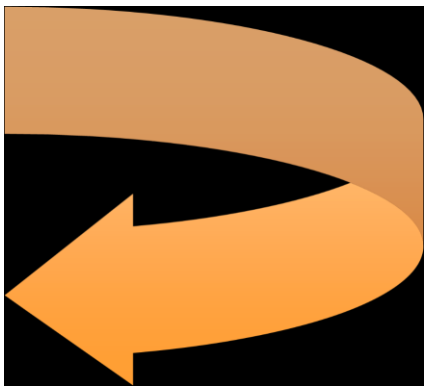


1. Orçamento limitado
2. Pouco tempo
3. Poucas pessoas
4. Pouco treino
5. Falta de suporte
6. Infraestrutura TI complexa
7. Equipa TI desqualificada
8. Falta de cooperação entre equipas
9. Politicas de segurança pouco definidas
10. Baixa maturidade de ferramentas TI
11. Infraestrutura TI mal concebida
12. Falta de colaboração entre equipas TI e Segurança

Luís Borges Gouveia, lmbg@ufp.edu.pt

Atitude de Segurança

- **Reativa**
  - Resposta a incidentes
  - Investigações
  - Aplicação de sanções
- **Preventiva**
  - Planeamento
  - Normalização
  - Infraestrutura segura
  - Educação e treino
  - Auditoria



Luís Borges Gouveia, lmbg@ufp.edu.pt

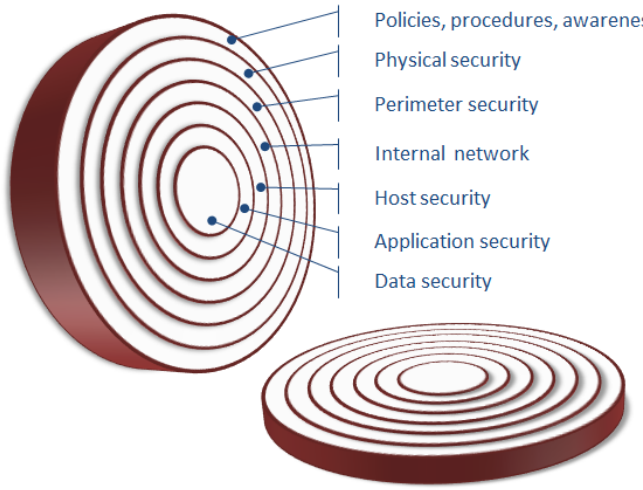
Medidas de Segurança

- Políticas
  - de segurança da informação
  - de utilização da Internet e Correio Electrónico
  - de instalação e utilização de software
- Plano de Classificação da Informação
- Auditoria(s)
- Análise
  - de Riscos
  - de Vulnerabilidades
  - de Políticas de Backup
- Plano de Ação Operacional
- Plano de Contingência
- Capacitação Técnica (formação e treino)
- Processo de Sensibilização dos Utilizadores

Medidas de Segurança

- *Backups* (rotinas de salvaguarda de informação)
- Antivírus
- *Firewall*
- Detecção de Intrusão (IDS)
- Servidor *Proxy*
- Filtros de Conteúdo
- Sistema de *Backup*
- Monitoração
- Sistema de Controle de Acessos
- Criptografia Forte
- Certificação Digital
- Teste de Invasão
- Segurança do acesso físico aos locais críticos

Controlo de segurança da informação por camadas



https://www.capgemini.com/blog/capping-it-off/2015/08/layering-information-security-controls

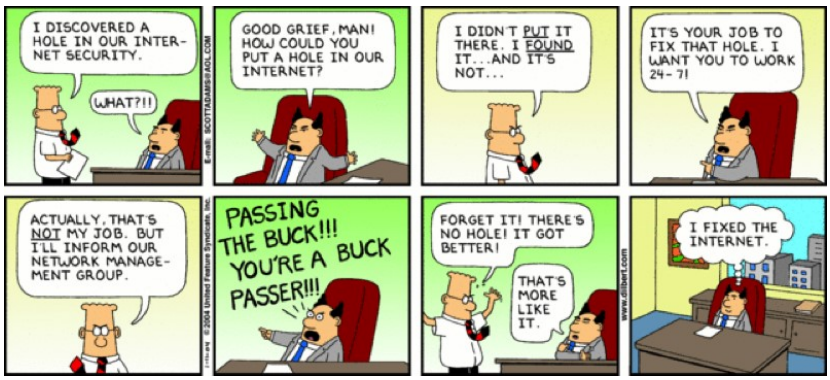
Principais Desafios

- Definição de Padrões e de Políticas
- Mudar a atitude sobre a segurança
- Demonstrar o retorno sobre o investimento em segurança
- Projecto de Segurança da Informação
- Projectos de proteção do negócio da empresa
- Fazer com que a Segurança da Informação seja um custo operacional
- Sensibilizar os executivos
- Motivar e treinar os utilizadores
- Capacitar a equipa técnica

Envolver e sensibilizar os decisores
(orçamento e preparação…)

Luís Borges Gouveia, lmbg@ufp.edu.pt

Envolver e sensibilizar os decisores
(mas também o seu conhecimento)



Luís Borges Gouveia, lmbg@ufp.edu.pt

Segurança da Informação

- *Como superar os desafios?*
- *Como implementar a Segurança da Informação?*
- *Como estabelecer controlos eficientes?*

Segurança da Informação

(tema atual e crítico para a sociedade, as organizações e os indivíduos)

Segurança da Informação

- Objetivo principal
  - Sensibilização para as questões da segurança da informação
    - O que é...
    - Conceitos...
    - Temas relevantes...
- Objetivos complementares
  - Apresentar normas e práticas correntes associadas com a doutrina nacional no quadro do uso de informação pública e/ou privada no contexto de defesa e segurança
  - Introduzir legislação aplicável
  - Analisar as implicações técnicas e sociais do tema

Luís Borges Gouveia, lmbg@ufp.edu.pt

Discussão de base tecnológica (informação digital) tendências da segurança da informação de 2015 a 2017

- Cibercrime
- Privacidade e regulação
- Ameaças originadas nos fornecedores
- BYOx (*bring-your-own device and/or application*) no local de trabalho
- Envolvimento e motivação dos trabalhadores
- *Ramsomware of things* (RoT)
- Educação para a segurança e responsabilidade social
- Segurança móvel (dispositivos móveis)
- Vulnerabilidades
- Próxima geração de software de segurança
- Desafios nos cuidados de saúde
- Ameaças às infraestruturas críticas
- Desafios e implicações da legislação de cibersegurança
- plataformas

http://www.cio.com/article/2857673/security0/5-information-security-trends-that-will-dominate-2015.html
http://www.welivesecurity.com/2017/01/04/year-security-trends-2017/

Luís Borges Gouveia, lmbg@ufp.edu.pt

Conceitos essenciais sobre segurança da informação

SEGURANÇA DA INFORMAÇÃO

Luís Borges Gouveia, lmbg@ufp.edu.pt

A atitude para com a segurança da informação

Um bom exemplo…

Provérbio Árabe

Luís Borges Gouveia, lmbg@ufp.edu.pt

A atitude para com a segurança da informação

Não digas tudo quanto sabes
não faças tudo quanto podes
não creias em tudo quanto ouves
não gastes tudo quanto tens

Luís Borges Gouveia, lmbg@ufp.edu.pt

A atitude para com a segurança da informação

porque
quem diz tudo quanto sabe
quem faz tudo quanto pode
quem crê em tudo quanto ouve
quem gasta tudo quanto tem

Luís Borges Gouveia, lmbg@ufp.edu.pt

A atitude para com a segurança da informação

muitas vezes
diz o que não convém
faz o que não deve
julga o que não vê
gasta o que não pode

Postura para a Segurança da Informação

"*The problem is not that there are problems.*

The problem is expecting otherwise and thinking that having problems is a ***problem****"*

O não existir problemas é que pode constituir um problema…

Theodore I. Rubin (1923,)

Conceito de segurança da informação

- Relacionada com proteção de um conjunto de dados, no sentido de preservar o seu valor (quer para o indivíduo, quer para a organização
- As suas caraterísticas básicas são os atributos de confidencialidade, integridade, disponibilidade e não repúdio
- Não restrita a Sistemas de Computador (informáticos), Informação de base eletrónica (digital) ou a sistemas de armazenamento e preservação de informação (arquivos físicos, digitais ou mistos)
- O conceito é aplicado a todos os aspectos de proteção de informação e dados. O conceito de *Segurança Informática* (mais alargado, a redes e sistemas) ou *Segurança de Computadores (associado com computadores)* está intimamente relacionado com o de Segurança da Informação, incluindo não apenas a segurança dos dados e informação, mas também a dos sistemas em si mesmos

Segurança da informação atributos: confidencialidade

- Propriedade que limita o acesso a informação tão somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação
  - Acesso a informação
  - Entidades legítimas
  - Autorização
  - Proprietário da informação

Segurança da informação atributos: integridade

- Propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controlo de mudanças e garantia do seu ciclo de vida (nascimento, manutenção e destruição)
  - Informação manipulada
  - Caraterísticas da informação
  - Controlo de mudanças
  - Ciclo de vida

Luís Borges Gouveia, lmbg@ufp.edu.pt

Segurança da informação atributos: disponibilidade

- Propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles utilizadores autorizados pelo proprietário da informação
  - Informação disponível
  - Uso legítimo
  - Utilizadores autorizados
  - Proprietário da informação

Luís Borges Gouveia, lmbg@ufp.edu.pt

Segurança da informação atributos: não repúdio

- Visa garantir que o autor não negue ter criado e assinado (ser origem) o documento
  - Autor da informação
  - Criação da informação
  - Assinatura da informação

  - Rastreabilidade
  - Verificalidade
  - Atribuição de origem

Ameaças à segurança (informação)

- As ameaças à segurança da informação são relacionadas directamente com a perda de qualquer uma das suas caraterísticas principais:
  - Perda de confidencialidade
  - Perda de integridade
  - Perda de disponibilidade

Perda de confidencialidade

- Ocorre quando há uma quebra de sigilo de uma determinada informação
  - exemplo: o par identificação e senha de um utilizador ou administrador de sistema
- Permite/leva a que seja exposta informação restrita, destinadas inicialmente a serem acessível apenas por um determinado grupo de utilizadores

Perda de integridade

- Acontece quando uma determinada informação fica exposta a manipulação por uma pessoa não autorizada, que efectua alterações que não foram aprovadas e não estão sob o controlo do proprietário (corporativo ou privado) da informação
  - Alteração
  - Eliminação
  - Acrescento
  - Inconsistência

Perda de disponibilidade

- Acontece quando a informação deixa de estar acessível por quem necessita dela
  - Por exemplo, no caso da perda de comunicação com um sistema importante para a empresa, por via de falha de um servidor ou de uma aplicação crítica de negócio
  - Causa falha ou erro por motivo interno ou externo ao equipamento ou por ação não autorizada de pessoas com ou sem má intenção

Níveis de segurança

- Depois de identificado o **potencial de ataque**, as organizações têm que decidir o **nível de segurança** a estabelecer para uma rede ou sistema (**contexto**), em função das **vulnerabilidade** detetadas, quais os **recursos físicos** e **lógicos** a necessitar de **proteção**
- No nível de segurança devem ser quantificados:
  - os **custos** associados aos **ataques** e
  - os **custos** associados à implementação de **mecanismos de proteção** para minimizar a sua **probabilidade de ocorrência** de um ataque
  - E também os custos de resolução das **vulnerabilidades** (caso tal seja possível)

Níveis de segurança e segurança física

Segurança física

- Considera as ameaças físicas como:
  - Incêndios
  - Desabamentos
  - Relâmpagos
  - Inundações
  - Acesso indevido de pessoas
  - Forma inadequada de tratamento e manuseamento do material
  - Implica desastres naturais, acidentes, erro humano e ações intencionais de desgaste, destruição ou vandalismo
- Muito associado com o controlo de acessos e o estabelecimento de perímetros de defesa
- Fator de dissuasão determinante para efeitos de segurança e segurança da informação

Luís Borges Gouveia, lmbg@ufp.edu.pt

Níveis de segurança e a segurança lógica

Segurança lógica

- Atenta contra ameaças ocasionadas por vírus, acessos remotos à rede, *backups* desatualizados, violação de senhas, etc.
- A segurança lógica é a forma como um sistema é protegido no nível de sistema operacional e de aplicação
  - Normalmente considerada como proteção contra ataques **mas** também significa proteção de sistemas contra erros não intencionais, como remoção acidental de ficheiros críticos de sistema ou de aplicação (o conceito de delimitação de perdas por erro humano)

Luís Borges Gouveia, lmbg@ufp.edu.pt

Mecanismos de segurança e controlos físicos

- São barreiras que limitam o contacto ou acesso directo a informação ou à infraestrutura (que garante a existência da informação) que a suporta
- Existem mecanismos de segurança que apoiam os controlos físicos:
  - *portas / fechaduras / paredes / blindagem / …*
  - *vigilância / guardas / sensores e actuadores / …*
- O efeito pode ser um ou vários dos seguintes:
  - Disuassão, de modo a inibir comportamentos não autorizados
  - Dificuldade de transpor perímetros, de modo a proteger acessos
  - Com o objetivo de tomar tempo, como forma de garantir tempo para reação ou ajuste de defesa
  - Com o objetivo de obter informação, como forma de perceber quem o faz, como o faz e quando o fez

Luís Borges Gouveia, lmbg@ufp.edu.pt

Mecanismos de segurança e controles lógicos

- Constituem barreiras que impedem ou limitam o acesso a informação, que está em ambiente controlado, geralmente eletrónico (e digital), e que, de outro modo, ficaria exposta a alteração não autorizada por elemento mal intencionado
- Existem mecanismos de segurança que apoiam os controlos lógicos:
  - *Criptografia, Assinatura Digital, Controlo de Acesso, Certificação, Protocolos Seguros, etc.*

Luís Borges Gouveia, lmbg@ufp.edu.pt

Políticas de segurança

- Uma política de segurança consiste num conjunto formal de regras que devem ser seguidas pelos utilizadores dos recursos de uma organização
  - Exige o seu cumprimento
  - Formação e sensibilização
  - Verificação e supervisão
- 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 direção
- Devem adaptar-se a alterações na organização, de forma rápida e não reactiva

Políticas de segurança

- Para a implantação de uma política de segurança devem ser considerado os seguintes princípios:
  - Disponibilidade
  - Utilização
  - Integridade
  - Autenticidade

Políticas de segurança
Disponibilidade

- O sistema deve estar disponível de forma que quando o utilizador necessitar, o possa usar
- Dados críticos devem estar disponíveis de forma permanente e ininterrupta
  - Acesso

Políticas de segurança
Utilização

- O sistema deve ser utilizado apenas para os objetivosdeterminados para a sua conceção (especificados para cada situação da empresa)
- As especificações pode ser orientadas de forma alternativa:
  - Orientado ao contexto
  - Orientado ao problema
  - Orientado à função

Políticas de segurança
Integridade

- O sistema deve estar sempre íntegro e em condições de ser usado
  - Obter resultados fiáveis
  - Obter resultados confiáveis
  - Obter resultados verdadeiros

Políticas de segurança
Autenticidade

- O sistema deve ter condições de verificar a identidade dos utilizadores, e este ter condições de analisar a identidade do sistema
  - Mecanismos de identificação como biometria e sensores são cada vez mais comuns
  - O uso de mecanismos de vigilância proporciona também formas de garantia de continuidade em tempo e qualidade para verificação a tempo real

Potencial para falhas de segurança

- Considerando os conceitos introduzidos, urge analisar a segurança da informação nas organizações e empresas
  - Como lidar com as pressões e vulnerabilidades causadas pela necessidade de colaboração de múltiplas organizações e comunidades que muitas das vezes possuem interesses sobrepostos ou conflituosos
- Deve ser tomado em linha de conta que actualmente, a grande maioria das informações disponíveis nas organizações se encontra armazenadas (em formato digital) e são trocadas entre os mais variados sistemas de computador e redes (muitas vezes abertas)

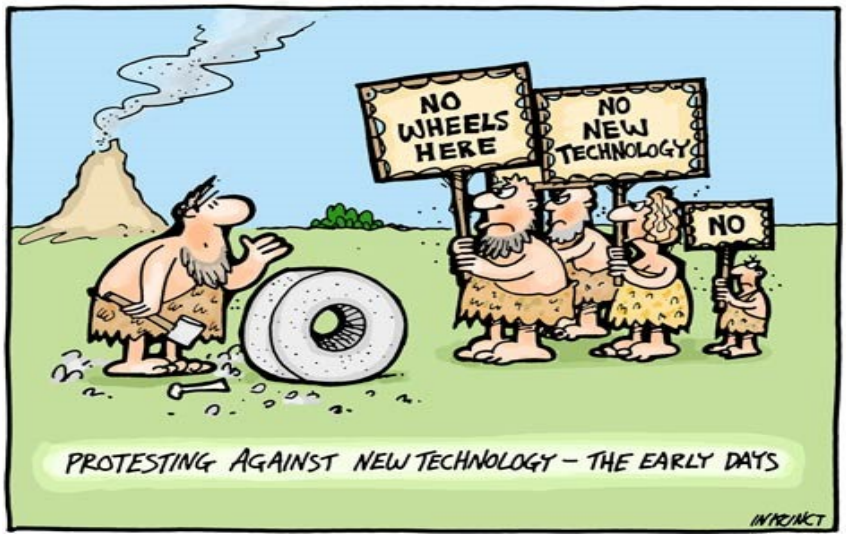
Propagação de erro e potencial de falha na segurança da informação

- Dessa forma, inúmeras vezes (mais do que as adequadas…) as decisões e ações tomadas decorrem de informações manipuladas por sistemas vulneráveis
  - Neste contexto, toda e qualquer informação deve ser correcta, precisa e estar disponível, a fim de ser armazenada, recuperada, manipulada ou processada, além de poder ser trocada de forma segura e confiável – qualidade da informação

O poder e dependência da informação

- É oportuno salientar que no contexto atual, a informação constitui uma mercadoria, ou até mesmo uma *commodity*, de importância crucial para as organizações, independentemente da sua dimensão ou tipo
- Por esta razão, a segurança da informação tem que ser considerada uma questão de elevada prioridade nas organizações e empresas (e não apenas no contexto da soberania, da segurança e defesa)
  - Por exemplo, a questão da qualidade também se pode enquadrar como uma questão de segurança da informação

Se a segurança da informação é novidade, então pode ter contestação na organização…



CICLO DE VIDA DA INFORMAÇÃO

Luís Borges Gouveia, lmbg@ufp.edu.pt

O ciclo de vida da informação

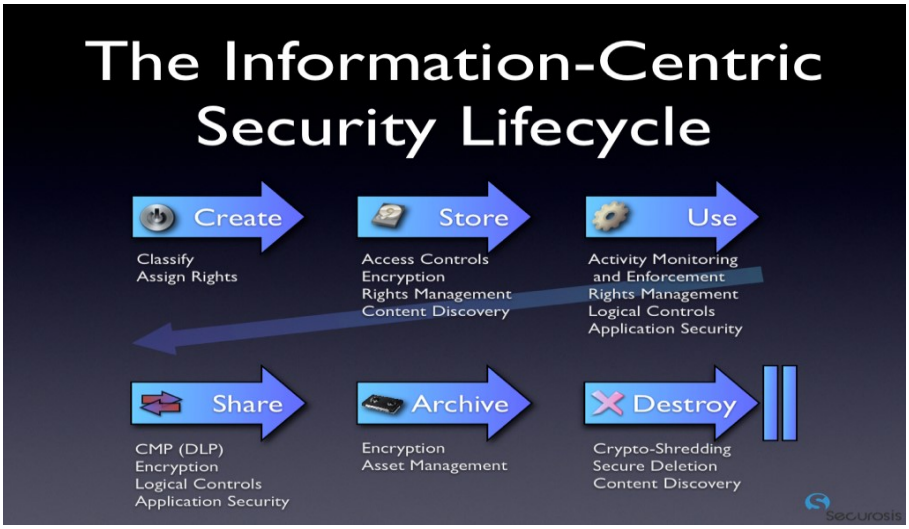
- O ciclo de vida da informação é composto e identificado pelos momentos vividos pela informação que a coloca em risco
  - Ocorre quando os ativos físicos, tecnológicos e humanos fazem uso da informação, nos processos da empresa que garantem o funcionamento desta

Luís Borges Gouveia, lmbg@ufp.edu.pt

Quatro momentos ou etapas do ciclo de vida da informação

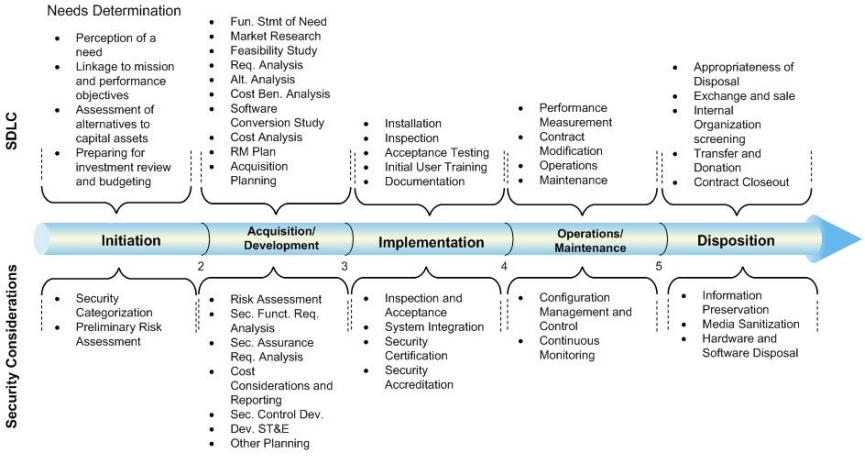
- Considerando o contexto da segurança da informação:
  - **Criação**: associado com a criação e uso da informação
  - **Armazenamento**: quando a informação é guardada ou registada para efeitos de posterior acesso e recuperação (quer em papel, quer no digital)
  - **Processamento**: inclui quatro grandes grupos de atividades (acesso, modificação, comunicação e visualização/impressão). Por exemplo, comunicação: quando a informação é transferida entre pontos de utilização (conversação telefónica, correio eletrónico ou circulação em papel dentro da empresa – correio interno – ou com o exterior)
  - **Destruição**: o descarte da informação corresponde à eliminação da informação e a sua destruição com colocação no lixo ou eliminação digital (meios simples e muitas vezes não definitivos)

Um exemplo (para o contexto da *cloud*)



A importância da metainformação

Segurança de dados (ciclo de vida)



http://www.guerilla-ciso.com/archives/270

Memória versus operação

"Information security is a major priority at this company.
We've done a lot of stupid things we'd like to keep secret."

Das ameaças e vulnerabilidades à análise de risco

A ANÁLISE DE RISCO

Princípios de qualidade da informação

- Segundo as normas de segurança da informação mais comuns
  - Integridade
  - Disponibilidade
  - Confidencialidade
- Mas também:
  - Continuidade de negócio
  - Relevância e valor
  - Rastreabilidade
    - Não repudiação
    - Autenticidade

Ameaças

- Potencial de desenvolvimento de incidentes que aproveitem a existência de vulnerabilidades existentes
- Tipos de ameaças em função da sua concretização
  - Episódicas
  - Permanentes
  - Intermitentes

Ameaças Acidentais (não intencionais)

- Causadas pelas forças da natureza
  - Inundações
  - Terramotos
  - Descargas elétricas
  - etc…
- Falhas de sistemas
  - Equipamento
  - Software
  - Comunicações
  - Energia elétrica

Ameaças Acidentais (não intencionais)

- Erros humanos
  - Desconhecimento (ignorância)
  - Falta de comunicação
  - Falta de treino
  - Relaxamento
  - Distração
- O erro humano são as ameaças mais habituais e as mais controláveis, por via da gestão de recursos humanos e da comunicação
  - Politicas de segurança da informação
  - Formação e treino
  - Sensibilização

Ameaças Causadas por Pessoas
(causas intencionais)

- Espionagem
- Crimes
- Empregados insatisfeitos
- Empregados "doentes"
- Empregados desonestos
- Vandalismo
- Terrorismo
- Erros dos Utilizadores

Danos causados

- A informação é:
  - Processada
  - Armazenada
  - Comunicada
- Os danos podem ser (acontecendo imediatamente, em tempo pré determinado ou ficam dormentes para ativação futura):
  - Permanentes
  - Transitórios
  - Intermitentes
- Tipos de impacto
  - Destruição de informação
  - Substituição de informação
  - Alteração/modificação de informação

Vulnerabilidades dos Computadores (a componente tecnológica do digital)

- Pequenos suportes guardam grandes volumes de dados (discos externos, USBs, etc.)
- Os dados são invisíveis e incorpóreos
- Os suportes podem falhar (com diferentes níveis de gravidade)
- Copiar não anula a informação (reproduz, sem controlo de original e cópia – nem de versões – por defeito)
- Avanços tecnológicos, complexidade, evolução, compatibilidade e compatibilidade

Luís Borges Gouveia, lmbg@ufp.edu.pt

Avaliação dos Riscos

- O que é um risco?
  - É uma relação entre o par ameaça / vulnerabilidade e o valor a proteger
  - É o produto da vulnerabilidade, multiplicada pela ameaça
  - Exige um contexto bem definido e conhecido
- O que é a análise de risco?
  - É o processo de avaliação, para um contexto específico da organização, se é ou não aceitável a probabilidade de ocorrência de concretização de uma ameaça para determinada vulnerabilidade

Luís Borges Gouveia, lmbg@ufp.edu.pt

Análise e avaliação de riscos

- $Risco = \frac{Ameaças * Vulnerabilidade * Impactos}{Medidas\ de\ Segurança}$
- Avaliação do risco:
  - Aplicar as medidas de segurança (resolver ou mitigar a situação com recurso a ação)
  - Aceitar o risco (opção consciente de não consideração)
  - Evitar o risco (lidar com este em meio de prevenção)
  - Transferir o risco (com recurso a seguros ou fornecedores)

Análise e medidas de segurança

- $Risco = \frac{Ameaças * Vulnerabilidade * Impactos}{Medidas\ de\ Segurança}$
- Medidas de segurança
  - Segurança física
  - Controlos tecnológicos
  - Segurança em software
  - Medidas organizacionais
  - Controle de acesso
  - Continuidade de negócio

Técnicas de Análise de Risco

- Desenvolver cenários de:
  - Ameaças
  - Vulnerabilidades
  - Considerando um (bem) determinado contexto
- Para cada cenário:
  - Listar os impactos e custos associados
  - Listar os recursos a envolver e as medidas a realizar para evitar o potencial incidente
  - Realizar uma análise de custo/benefício

Técnicas de Análise de Risco

- Análise subjetiva
  - Estudo individual ou coletivo realizado por um conjunto de profissionais da organização ou por uma sua equipa de segurança, com base em cenários desenvolvidos em sessões de *brainstorming* ou do tipo *card sorting*
- Análise quantitativa
  - Mais estruturada e baseada numa aproximação baseada em processos, tomando cada vulnerabilidade identificada:
    - Para cada **ameaça**: quantificar a sua probabilidade de ocorrência
    - Estimar o valor do **impacto** e prejuízos que pode causar
    - Estimar o custo de combater a ameaça – **medida**
  - Pesar as várias ameaças para obter um valor final
    - Qual o algoritmo usar para quantificar o seu valor?

Técnicas de Análise de Risco

- Técnicas automatizadas
  - Uso de ferramentas informáticas que implementam um algoritmo específico
  - Dois exemplos:
    - CRAMM (Reino Unido): método que utiliza a ferramenta CCTA *Risk Analysis and Management Method*
    - ISSO/IEC 27001 (ISO): *Information security management systems – Requirements* (norma orientada para o processo de certificação)
- *Listagem de métodos de análise de risco, fornecida pela ENISA: http://rm-inv.enisa.europa.eu/methods*
- *Ferramentas de apoio à análise de risco: http://rm-inv.enisa.europa.eu/tools*

CRAMM, 3 etapas (gestão de risco)

- Etapa 1: identificação de riscos
  - Identificação dos recursos a proteger, custo, grau de criticidade da sua indisponibilidade, ...
- Etapa 2: análise de riscos
  - Avaliação das vulnerabilidades do sistema (o CRAMM considera 31 tipos de ameaças)
  - São usados questionários aos profissionais envolvidos, para fazer uma avaliação ponderada
- Etapa 3: avaliação de riscos
  - Usa um algoritmo e faz recomendações sobre os recursos a proteger, medidas a tomar

ISO 27001, 3 etapas (gestão de risco)

- Etapa 1: avaliação de risco
  - Requisito genérico que a avaliação de risco tem de ser realizada de acordo com um método credível e reconhecido (não especificado)
- Etapa 2: tratamento do risco
  - Recomendação genérica da necessidade de que o risco tem de ser tratado
- Etapa 3: aceitação do risco
  - Considerado de forma indireta através da especificação de aplicabilidade

Vulnerabilidades do Software

- Falhas do sistema operativo
  - Especificações e personalização
  - Instalação e operação
  - Manutenção e suporte
- Falhas de aplicações
  - Especificações
  - Desenvolvimento
  - Implementação
  - Manutenção
  - Integração

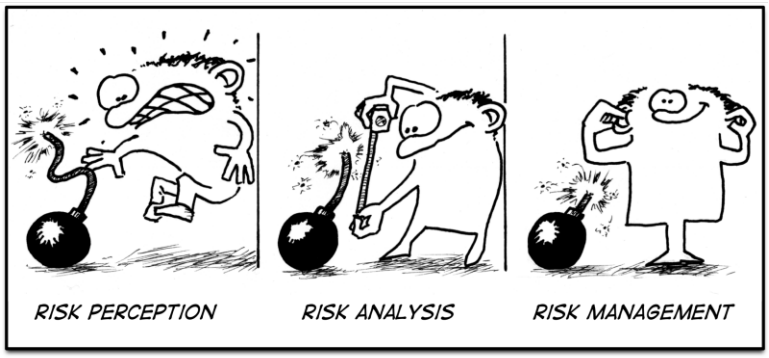
CERT (*Computer Emergency Response Team*)

- Estrutura organizada para a recolha e divulgação de incidentes e ocorrências de eventos relacionados com a segurança da informação, da cibersegurança e da informática
- Cadeia segura de troca de informação
  - Falhas de sistema operativo
  - Falhas de aplicações
  - Vírus e outro software malicioso
  - Ataques e técnicas ofensivas e de exploração ciber

Exemplos de CERTs

- CERT.PT – *Serviço de Resposta a Incidentes de Segurança Informática*
  - *http://www.cert.pt/*
- ENISA – *European Union Agency for Network and Information Security*
  - *http://www.enisa.europa.eu/*
- US-CERT – *United States Computer Emergency Readiness Team*
  - *http://www.us-cert.gov/*

A análise de risco tem de ter seguimento…



http://environmentalrisk.org/dont-touch-this-button/

Tipos de informação de acordo com a sua confidencialidade

CLASSIFICAÇÃO DA INFORMAÇÃO

Contexto

- No contexto da Sociedade da Informação e da crescente importância da informação, importa salvaguardar o seu uso e proteger dados e informação de modo a preservar também o seu valor
- Deste modo, as preocupações com a segurança são importantes e a norma ISO 27000 constitui a principal família de normas para a segurança da informação
  - É apresentada a classificação de informação de acordo com a sua confidencialidade
  - A norma está apoiada nos princípios da integridade, disponibilidade e confidencialidade da informação

Luís Borges Gouveia, lmbg@ufp.edu.pt

Processo de classificação da informação

- Possui quatro etapas
  1. Identificar a informação como um ativo a inventariar
  2. Classificação da informação
  3. Rotulagem da informação
  4. Manipulação e manuseio da informação
- Para a operacionalização destas quatro etapas é desenvolvida uma política de classificação da informação

Luís Borges Gouveia, lmbg@ufp.edu.pt

Processo de classificação da informação
1. Inventário de ativos (registo de ativo)

- O objetivo do esforço de desenvolvimento de um inventário de ativos é para obter uma lista exaustiva de quais os itens de informação que devem ser classificados e quem é responsável por cada um deles (o seu dono)
- A informação classificada pode estar em diferentes formatos e tipos de media, como por exemplo:
  - Documentos eletrónicos
  - Sistemas de informação / bases de dados
  - Documentos em papel
  - Meios de armazenamento (discos, usb, etc.)
  - Informação transmitida verbalmente
  - Correio eletrónico (*email*)

Processo de classificação da informação
2. Classificação de informação

- A ISO 27001 não prescreve os níveis de classificação
  - permite a liberdade de adotar o que é mais comum no país ou setor da indústria
- Quanto maior e mais complexa a organização, mais níveis de confidencialidade terá
- Por exemplo, para organizações de média dimensão, podem ser considerados 4 níveis de classificação da informação, com três níveis de confidencialidade e um nível público:
  - **Confidencial** (o mais alto nível de confidencialidade)
  - **Restrita** (médio nível de confidencialidade)
  - **Uso interno** (o mais baixo nível de confidencialidade)
  - **Pública** (todos podem ver a informação)
- Em muitos casos, o dono do ativo é o responsável por classificar a informação, o que é feito com base nos resultados da análise/avaliação de riscos:
  - quanto maior o valor da informação (amplifica as consequências de uma quebra da confidencialidade), maior deveria ser o nível de classificação

Processo de classificação da informação
2. Classificação de informação

- É frequente uma organização dois ou mais esquemas de classificação diferentes implantados
  - Por exemplo, no caso de trabalhar tanto como o setor governamental, quanto com o privado
- Um exemplo é a NATO, que classifica a informação em seis níveis, com quatro níveis de confidencialidade restrita e dois níveis públicos:
  - Altamente secreto (*Cosmic **Top Secret***)
  - NATO Secreto (*NATO **Secret***)
  - NATO Confidencial (*NATO **Confidential***)
  - NATO Restrito (*NATO **Restricted***)
  - NATO Não Classificado (direito autoral) (*NATO Unclassified* (**copyright**))
  - Informação não sensível, de domínio público (*Non sensitive information releasable to the **public***)

Processo de classificação da informação
3. Rotulagem da informação

- Uma vez classificada a informação, é necessário proceder à sua rotulagem
  - Desenvolver orientações para cada tipo de ativo de informação sobre como ele precisa ser rotulado (a ISO 27001 não prescreve soluções ficas, pelo que devem ser desenvolvidas regras próprias)
- Por exemplo, definir as regras para documentos em papel de forma a que:
  - o nível de confidencialidade seja indicado no canto superior direito de cada página do documento,
  - a classificação da informação seja indicada na capa ou no envelope que transporta o documento
  - E também colocada a classificação na pasta onde o documento é armazenado
- A rotulagem da informação é geralmente da responsabilidade do proprietário da informação

Processo de classificação da informação
4. Manipulação e manuseio de ativos

- A parte mais complexa do processo de classificação
- Consiste no desenvolvimento de regras sobre como proteger cada tipo de ativo, dependendo do seu nível de confidencialidade
  - Organizar uma tabela com a listagem de ativos e o seu nível de confidencialidade e com indicação das medidas associadas
  - Exemplo: definir que um documento em papel, classificado como restrito, deve ser guardado em espaço próprio (cofre/armário fechado); ou que documentos podem ser transferidos dentro e fora da organização, apenas em envelope fechado e no caso de ser enviado para fora da organização, o documento deve ser enviado com registo ou em mão própria, com registo prévio dos ativos manipulados

Processo de classificação da informação
4. Manipulação e manuseio de ativos

- A ISO 27001 permite definir as próprias regras, geralmente definidas na política de classificação da informação, ou nos procedimentos de classificação
  - O processo de classificação pode ser complexo, mas tem de ser claro e facilmente aplicável, de forma a ser seguido
  - Também neste contexto, a ISO 27001 dá uma grande liberdade, permitindo adaptar um processo a necessidades especiais, de forma a assegurar que informação sensível esteja protegida

A normalização em Segurança da Informação

NORMAS E PROCEDIMENTOS

Luís Borges Gouveia, lmbg@ufp.edu.pt

Normas para a gestão de segurança da informação

- RFC 2196: *Site Security Handbook* (IETF)
- BS 7799 *Information Security Management* (*British Standards Institute*): http://www.c-cure.org
  - BS 7799-1 *Code of Practice for ISM* (*Information Security Management*)
  - BS 7799-2 *Specifications for ISM Systems*
- ISO/IEC 17799:2005 *Information technology – Security techniques – Code of practice for information security management*
- ISO/IEC 27001:2005 *Information technology – Security techniques – Information security management systems – Requirements*

Luís Borges Gouveia, lmbg@ufp.edu.pt

RFC 2196 (*request for comments 2196*)

http://tools.ietf.org/html/rfc2196

http://www.c-cure.org/7799Overview.htm

Home

What is it?
Register now
DISC's role
FAQs
What's New
Guides
Training
BS 7799
Contact Info
Taxonomy
Certification
Organisations
Auditors
Consultants
Committee

BS ISO/IEC 17799:2000 - Overview

What is information security?

Information is an asset which, like other important business assets, has value to an organization and consequently needs to be suitably protected. Information security protects information from a wide range of threats in order to ensure business continuity, minimize business damage and maximize return on investments and business opportunities.

Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation. Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected.

Information security is characterized in the standard as the preservation of:

- Confidentiality
- Integrity
- Availability

Information security is achieved by implementing a suitable set of controls, which could be policies, practices, procedures, organizational structures and software functions. These controls need to be established to ensure that the specific security objectives of the organization are met.

Why information security is needed

A família de normas ISO 2700x (*Information technology – Security techniques*, *http://www.iso.org*)

- **ISO/IEC 27000:2014**
  - Information security management systems – Overview and vocabulary
- **ISO/IEC 27001:2013**
  - Information security management systems – Requirements
- **ISO/IEC 27002:2013**
  - Code of practice for information security controls
- **ISO/IEC 27003:2010**
  - Information security management system implementation guidance
- **ISO/IEC 27004:2009**
  - Information security management -- Measurement
- **ISO/IEC 27005:2011**
  - Information security risk management
- **ISO/IEC 27006:2015**
  - Requirements for bodies providing audit and certification of information security management systems
- **ISO/IEC 27010:2015**
  - Information security management for inter-sector and inter-organizational communications
- **ISO/IEC 27019:2013**
  - Information security management systems -- Overview and vocabulary

Normas de Gestão de Segurança

- ISO 20000
  - Parte 1: ISO/IEC 20000-1:2005 - Especificação (Preparada pelo BSI - *British Standard Institute* - como BS 15000-1)
  - Parte 2: ISO/IEC 20000-2:2005 - Código de Boas Práticas (Preparada pelo BSI como BS 15000-2)
- ITIL (norma associada com a infraestrutura de TI - Tecnologias de Informação e com os Sistemas de Informação)
  - *IT Govenance Institute* - *http://www.itgi.org/*

Normas de Gestão de Segurança

- Manual de proteção de TI
  - Alemanha (*Baseline Protection Catalogs – IT-Grundschutz-Kataloge*) 10/2000 IT
  - **Information Warfare site:** *http://www.iwar.org.uk/comsec/resources/standards/germany/itbpm/menue.htm*

Luís Borges Gouveia, lmbg@ufp.edu.pt

Baseline Protection Manual

- **1 Finding Your Way Around the IT Baseline Protection Manual**
- 1.1 IT Baseline Protection: The Aim, Concept and Central Idea
- 1.2 Structure and Interpretation of the Manual
- 1.3 Using the IT Baseline Protection Manual
- 1.4 Brief Outline of Existing Modules
- 1.5 Additional Aids
- 1.6 Information Flow and Points of Contact
- **2 Using the IT Baseline Protection Manual**
- 2.1 IT Structure Analysis
- 2.2 Assessment of protection requirements
- 2.3 IT Baseline Protection Modelling
- 2.4 Basic Security Check
- 2.5 Supplementary Security Analysis
- 2.6 Implementation of IT Security Safeguards
- 2.7 IT Baseline Protection Certificate
- **3 IT Baseline Protection of Generic Components**
- 3.0 IT Security Management
- 3.1 Organisation
- 3.2 Personnel
- 3.3 Contingency Planning Concept
- 3.4 Data Backup Policy
- 3.5 Data Privacy Protection
- 3.6 Computer Virus Protection Concept
- 3.7 Crypto Concept
- 3.8 Handling of Security Incidents
- **4 Infrastructure**
- 4.1 Buildings
- 4.2 Cabling
- 4.3 Rooms
- 4.3.1 Offices
- 4.3.2 Server Rooms
- 4.3.3 Storage Media Archives
- 4.3.4 Technical Infrastructure Rooms
- 4.4 Protective Cabinets
- 4.5 Working Place At Home (Telecommuting)
- 5 **Non-Networked Systems**
- 5.1 DOS PC (Single User)
- 5.2 UNIX System
- 5.3 Laptop PC
- 5.4 PCs With a Non-Constant User Population
- 5.5 PC under Windows NT
- 5.6 PC with Windows 95
- 5.99 Stand-Alone IT Systems Generally
- 6 **Networked Systems**
- 6.1 Server-Supported Network
- 6.2 UNIX Server
- 6.3 Peer-to-Peer Network
- 6.4 Windows NT Network
- 6.5 Novell Netware 3.x
- 6.6 Novell Netware 4.x
- 6.7 Heterogeneous Networks
- 6.8 Network and System Management
- 7 **Data Transmission Systems**
- 7.1 Exchange of Data Media
- 7.2 Modem
- 7.3 Firewall
- 7.4 E-Mail
- 7.5 WWW Server
- 7.6 Remote Access
- 8 **Telecommunications**
- 8.1 Telecommunications System (Private Branch Exchange, PBX)
- 8.2 Fax Machine
- 8.3 Answering Machine
- 8.4 LAN connection of an IT system via ISDN
- 8.5 Fax Servers
- 8.6 Mobile Telephones
- 9 **Other IT Components**

Luís Borges Gouveia, lmbg@ufp.edu.pt

Baseline Protection Manual

http://www.iwar.org.uk/comsec/resources/standards/germany/itbpm/etc/inhalt.htm

- Standard Software
- 9.2 Databases
- 9.3 Telecommuting

Catalogues of Safeguards **(salvaguardas/medidas)** ***and Threats*** **(ameaças)**

• **Safeguards Catalogues**	**Threats Catalogues**
• S 1 Infrastructure	T 1 Force Measure
• S 2 Organisation	T 2 Organisational Shortcomings
• S 3 Personnel	T 3 Human Error
• S 4 Hardware & Software	T 4 Technical Failure
• S 5 Communication	T 5 Deliberate Acts
• S 6 Contingency planning	

Luís Borges Gouveia, lmbg@ufp.edu.pt

Normas de Gestão de Segurança

- **OCDE –** ***Organization for Economic Co-operation and Development***
  - *Guidelines for the Security of Information Systems and Networks: towards a Culture of Security (2002)* http://www.oecd.org/document/42/0,3343,en_2649_34255_15582250_1_1_1_1,00.html

OECD ***Organisation for Economic Co-operation and Development***

Luís Borges Gouveia, lmbg@ufp.edu.pt

Normas de avaliação de segurança

- ISO 15408 (*Common Criteria for Information Technology Security Evaluation*) – família de normas de 2008 e 2009
  - *baseado na ITSEC (UK i90), Canadian Criteria, US Federal Criteria (esta, inspirada no ITSEC i90)*
- *Trusted Computer System Evaluation Criteria / 85 (TCSEC ou Orange Book* DoDD 5200.28-STD, já descontinuado*) – Rainbow Series*
  - é a base para avaliar e selecionar sistemas de computador considerados para processamento, armazenamento e recuperação de informação sensível e classificada
- *CoBIT – Control Objectives for Information and related Technology* http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx
  - *Information Systems Audit and Control Association®*

Normas para o desenvolvimento de aplicações informáticas

- SEI – *Software Engineering Institute* (*http://www.sei.cmu.edu/*)
  - CMM: *Capability Maturity Model*
  - CMMI: *Capability Maturity Model Integrated* (*http://www.sei.cmu.edu/cmmi/*)

Software Engineering Institute

Normas para o desenvolvimento de aplicações informáticas

- SSE-CMM: *System Security Engineering – Capability Maturity Model (http://www.sse-cmm.org)*
  - *modelo para o processo de engenharia e segurança de uma organização (http://www.sse-cmm.org/docs/ssecmmv3final.pdf)*

Normas para serviços financeiros

- ISO 11131 – *Banking and Related Financial Services – Sign-On Authentication*
  - descontinuado e substituido… ver http://www.iso.org/iso/catalogue_detail.htm?csnumber=19150
- ISO/TR 13569:2005 – *Financial services – Information security guidelines*

Normas para serviços de saúde

- *Information Security Program Policy US Department of Health and Human Services* (relatório)
  - *http://www.samhsa.gov/IT/Docs/Information_Security_Program_Policy_07192005.pdf*
- *ISO 27799:2013 Health informatics*
  - *Information security management in health using ISO/IEC 27002*
- *ISO 20302:2014 Health informatics*
  - *Health cards – Numbering system and registration procedure for issuer identifiers*
- *ISO 22857:2013 Health informatics*
  - *Guidelines on data protection to facilitate trans-border flows of personal health information*

Normas para serviços de saúde

- *ISO/TS 21547:2010*
  - *Health informatics – Security requirements for archiving of electronic health records – Principles*
- *ISO/TR 11633-1:2009*
  - *Health informatics – Information security management for remote maintenance of medical devices and medical information systems -- Part 1: Requirements and risk analysis*
- *ISO/TR 11633-2:2009*
  - *Health informatics – Information security management for remote maintenance of medical devices and medical information systems -- Part 2: Implementation of an information security management system (ISMS)*

Normas e recomendações nacionais

- Comissão Nacional de Proteção de Dados - http://www.cnpd.pt/
  - Legislação Nacional: http://www.cnpd.pt/bin/legis/leis_nacional.htm
- Normas gerais de segurança nacionais (PT) – SEGNAC (antigo) http://www.cfsirp.pt/index.php?option=com_content&task=view&id=87&Itemid=34
  - SEGNAC 1: regras sobre tipos de informação e matérias classificadas,
  - SEGNAC 2: segurança industrial
  - SEGNAC 3: segurança das comunicações
  - SEGNAC 4: segurança informática.

Norma BS – 7799:2002

- SGSI – Sistema de Gestão de Segurança da Informação
  - Componentes princípais de um SGSI
  - Estabelecimento de um SGSI
  - Implementação de um SGSI
  - Monitorização e revisão de um SGSI
  - Manutenção e melhoramento de um SGSI

ISO/IEC 18028-4:2005

Segurança da Informação

- definida na norma como ***a preservação da confidencialidade, integridade e disponibilidade***
  - **Confidencialidade**: assegurar que só pessoas autorizadas possam aceder à informação
  - **Integridade**: assegurar que a informação e os métodos para o seu processamento são exactos e completos
  - **Disponibilidade**: assegurando que os utilizadores autorizados tem acesso à informação quando o pretendem ou necessitam

As 10 áreas de controle na norma ISO/IEC 18028-5:2006 (descontinuada)

Information technology -- Security techniques -- IT network security -- Part 5: Securing communications across networks using virtual private networks

Atualmente, norma substituida por ISO/IEC 27033-5:2013

- Políticas de segurança corporativa ou empresarial
- Organização da segurança
- Classificação e controlo de activos
- Segurança de pessoal
- Segurança física e ambiental
- Administração de operações e comunicação
- Controlo de Acceso
- Desenvolvimento e manutenção de sistemas
- Planos de continuidade de negócio (BCP – *business continuity plan*) / Planos de recuperação e contingência (DRP – *data recovery plan*)
- Cumprimento dos requisitos legais (no caso da informação e no contexto nacional, especial atenção à LPD – Lei de Proteção de Dados e à CNPD – Comissão Nacional de Proteção de Dados)

A norma ISO 27001:2013 possibilita:

- Conceber uma ferramenta para a implementação de um sistema de gestão de segurança de informação, tomando em consideração políticas, a estrutura organizacional, os procedimentos e os recursos
- A gestão das políticas e dos objetivos de segurança em termos de integridade, confidencialidade e disponibilidade, pelos responsáveis da organização
- Determinar e analisar os riscos, identificando ameaças, vulnerabilidades e impactos na atividade empresarial
- Prevenir ou reduzir, de forma eficaz, o nível de risco por via da implementação de controlos adequados, preparando a organização para potenciais emergências e garantindo a continuidade de negócio

Luís Borges Gouveia, lmbg@ufp.edu.pt

Etapas associadas com a certificação de Gestão de Segurança da Informação

- Planificação
  - é realizada uma análise documental (avaliação de riscos, políticas, abrangência, declaração de aplicabilidade e processos) de acordo com os requisitos especificados pela norma ISO 27001
- Auditoria
  - a equipa de auditoria comprova se a implementação do sistema de gestão de segurança da informação é eficaz para a organização
- Certificação
  - é atribuída a certificação ISO 27001, por um período de tempo (três anos)
- Seguimento
  - são efectuados auditorias de seguimento de modo a verificar se são mantidas as condições e os requisitos que permitiram a obtenção da certificação pela empresa.

Luís Borges Gouveia, lmbg@ufp.edu.pt

Sistema de Gestão da Segurança
(*Information Technology – Security techniques)*

ISO/IEC 2700X

Luís Borges Gouveia, lmbg@ufp.edu.pt

A família ISO 27000: 2016

- 4ª versão – 15 de Fevereiro de 2016
  Information technology — Security techniques — Information security management systems — Overview and vocabulary
- Disponível em pdf em
  http://standards.iso.org/ittf/PubliclyAvailableStandards/c066435_ISO_IEC_27000_2016(E).zip

A norma ISO/IEC 27001:2013

- ISO/IEC 27001:2013 *"Information technology – Security Techniques – Information Security Management Systems (ISMS) – Requirements*".
- Apresenta um modelo para o estabelecimento, operação, monitorização, revisão, manutenção e melhoria de um sistema de gestão de segurança da informação de uma organização.
  - Em conformidade com as recomendações especificadas na norma ISO/IEC 17799:2005 (descontinuada)
  - Baseado na norma desenvolvida pelo BSI - *British Standards Institution* como BS 7799-2

Norma ISO/IEC 27001:2013

- Integra uma família de normas sobre segurança da informação para suportar e orientar a proteção de activos de informação na área das tecnologias de informação e comunicação
  - ISO/IEC 27000 *Fundamentals and Vocabulary*
  - ISO/IEC 27001 *ISMS Requeriments*
  - ISO/IEC 27002 *Code of practices for information security management*
  - ISO/IEC 27003 ISMS *Implementation Guidance*
  - ISO/IEC 27004 *Information Security Management Measurement*
  - ISO/IEC 27005 *Information Security Risk Management*

A norma ISO/IEC 27001:2013

- O que é um Sistema de Gestão de Segurança da Informação (SGSI, em Inglês, ISMS)?
  - Estabelece as políticas de segurança da informação de uma organização e dos seus objetivos
  - Especifica como alcancar os objetivos pretendidos
  - Estrutura organizacional
  - Planificação de atividades
  - Responsabilidades
  - Práticas, procedimentos e processos
  - Recursos
  - Estabelece uma série de documentos obrigatória para efeitos de certificação

Modelo baseado em processos

- Uma qualquer atividade (de segurança da informação) que emprega recursos para
  - Transformar entradas em saídas (objetivos de segurança)
  - O processo de gestão de segurança da informação é desenvolvido seguindo o modelo PDCA
  - O conceito de processo é transversal aos sistemas de qualidade, aos sistemas de informação e ao utilizado no contexto da norma de segurança da informação

Entender as normas – documentos

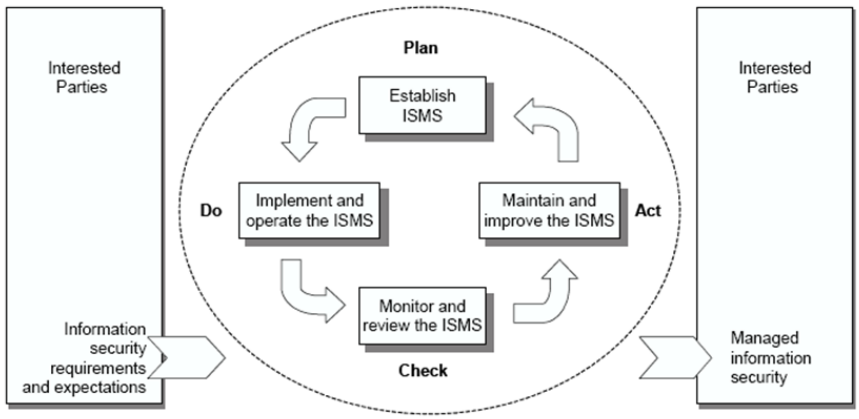
- A maior parte das normas (tal como as normas 27000) possuem os seguintes documentos:
  - **Requisitos**: associados com o "tem" (requisitos obrigatórios) e que constituem os requisitos a implementar a não ser que haja exceções específicas. O auditor irá apenas auditar com base nos requisitos destes "tem" – requisitos obrigatórios
  - **Código de conduta**: estes são os "deve" (requisitos opcionais) e serve de guia à sua implementação
  - **Guias de orientação**: uma norma completa e praticável que não possui um esquema de certificação. É possivel estar em conformidade com a norma, mas não certificado

Modelo Plan-Do-Check-Act (PDCA) de 4 fases

- Planear (*plan*):
  - planear e estabelecer o SGSI*
- Fazer (*do*):
  - implementar e operacionalizar o SGSI*
- Verificar (*check*):
  - monitorizar e rever o SGSI*
- Agir (*act*):
  - manter e melhorar o SGSI*

* SGSI: Sistema de Gestão de Segurança de Informação (ISMS, em Inglês)

Modelo Plan-Do-Check-Act (PDCA)



PLANEAR: estabelecer o SGSI

- Definir o contexto do SGSI e as políticas de segurança da organização
- Identificar e realizar uma análise de risco dos ativos de informação relevantes
- Selecionar os objetivos de controlo e os controlos relevantes para a manipulação de riscos.
- Preparar o documento de aplicação e viabilidade da norma
- Atenção ao cumprimento da norma que debe estar de acordo com os requisitos especificados, nomeadamente nos aspectos mais essenciais e nas prioridades enunciadas para o SGSI

FAZER: implementar e operacionalizar o SGSI

- Implementar os controles (processos, procedimentos, tecnologia e sensibilização dos recursos humanos) para minimizar os riscos e cumprir com os objetivos de controle, anteriormente especificados

VERIFICAR: monitorizar e rever o SGSI

- Rever de forma periódica a eficiência do SGSI (políticas, processos, procedimentos, tecnologia e formação)
- Rever os níveis de risco aceitável e de risco residual
- Realizar as auditorias internas e externas ao SGSI

AGIR: manter e melhorar o SGSI

- Executar ações preventivas e correctivas para a melhoria contínua do SGSI
- Validar as propostas e ações de melhoria

Luís Borges Gouveia, lmbg@ufp.edu.pt

Benefícios da implementação da ISO 27001

- Conformidade
- Efeito de marketing
- Diminuição de despesas
- Aumento de confiança para parceiros
- Ordenar e sistematizar o negócio e o seus sistemas de informação
- Colocar a discussão da segurança da informação em foco, na organização

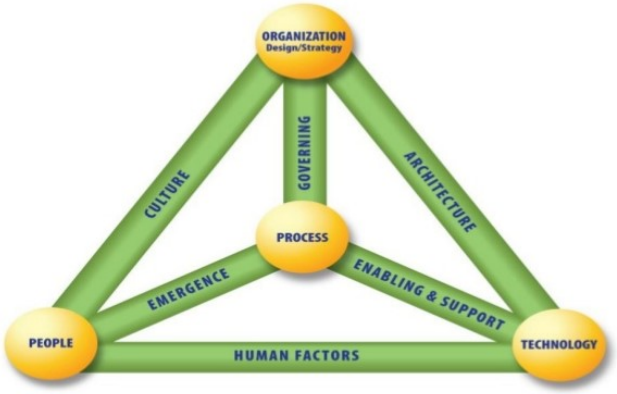
Luís Borges Gouveia, lmbg@ufp.edu.pt

Assegurar a continuidade de revisão do SGSI

CERTIFICAÇÕES EM SEGURANÇA DA INFORMAÇÃO

Segurança da informação (CBK – *Common body of knowledge, http://www.isc2.org*)

- A segurança da informação é a prática de defesa da informação do acesso não autorizado, do uso, da sua divulgação, de destruição, da modificação, do mau uso, da inspeção, do registo ou da destruição



Luís Borges Gouveia, lmbg@ufp.edu.pt

Certificação em Segurança da informação

- A avaliação compreensiva dos controlos de segurança técnicos e não técnicos de um sistema de tecnologias de informação para suporte do processo de acreditação que estabelece o grau com que uma conceção e implementação cumpre um conjunto específico de requisitos de segurança
  - Certificação profissional de indivíduos
  - Certificação das organizações
  - Certificação de sistemas de hardware
  - Certificação de sistemas de software
  - Certificação de instalações informáticas

Luís Borges Gouveia, lmbg@ufp.edu.pt

Certificação profissional em Segurança da informação

- Certificação profissional
  - Avalia e certifica o conhecimento e a sua atualidade no contexto da segurança da informação
- Para quem pretender abraçar uma carreira profissional enquanto especialista na área da segurança da informação, a certificação é uma mais valia
  - Permite verificar a existência de conhecimento especializado e atual sobre o tema ou partes específicas do tema da segurança da informação
  - Normalmente associado a exames e provas de competência
  - Existe material de estudo que pode ser obtido e que está relacionado com a preparação dos exames de certificação

As 5 certificações mais valorizadas

- Para quem pretender abraçar uma carreira profissional enquanto especialista na área da segurança da informação, a certificação é uma mais valia
  - *CompTIA Security + https://certification.comptia.org*
  - *Certified Ethical Hacker (CEH) https://www.eccouncil.org/*
  - *GIAC Security Essentials (GSEC) http://www.giac.org/*
  - *Certified Information Systems Security Professional (CISSP): Architecture (CISSP-ISSAP); Engineering (CISSP-ISSEP); Management (CISSP-ISSMP) https://www.isc2.org*
  - *Certified Information Security Manager (CISM) http://www.isaca.org/*

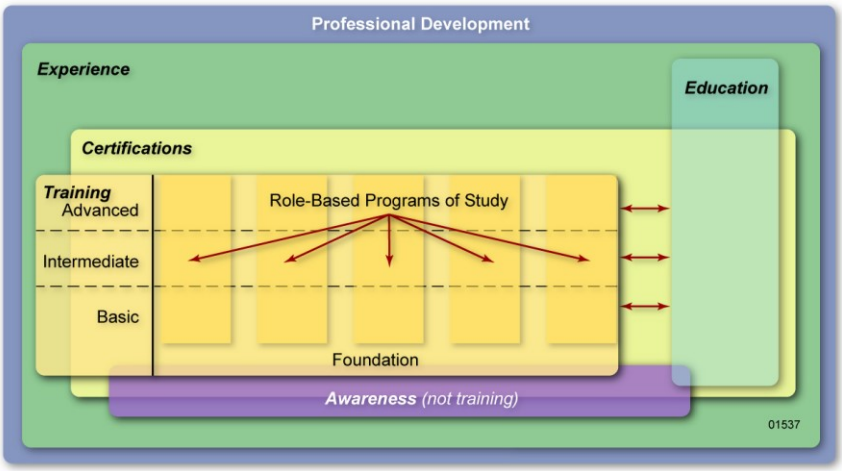
Outras certificações procuradas

- *Information Systems Security Engineering Professional (ISSEP/CISSP)*
- *EC-Council Licensed Penetration Tester Consultant*
- *EC-Council Licensed Penetration Tester Engineer*
- *GIAC Certified Penetration Tester*
- *GIAC Security Essentials*
- *Cybersecurity Forensic Analyst*
- *EC-Council Certified Secure Programmer*
- *Check Point Certified Security Expert*
- *Certified Secure Software Lifecycle Professional*

5 propostas de formação profissional avançada em segurança da informação

- *Certified Information Systems Security Professional (CISSP), (ISC)2 http://www.isc2.org/*
- *Systems Security Certified Practitioner (SSCP), (ISC)2 http://www.isc2.org/*
- *Certified Information Systems Auditor (CISA), ISACA http://www.isaca.org/*
- *Certified Information Security Manager (CISM), ISACA http://www.isaca.org/*
- *Global Information Assurance Certification (GIAC), SANS Institute http://www.giac.org/*

A formação e treino em segurança da informação é mais do que a certificação



NIST (2006). Information Security Handbook: a guide for managers.
http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf

Luís Borges Gouveia, lmbg@ufp.edu.pt

Sensibilização para a segurança

- Proporcionar um entendimento da importância da segurança internamente à organização
- Informar os trabalhadores acerca dos seus papeis e das expetativas que lhes estão associadas, de acordo com os requisitos de segurança da informação
- Proporcionar orientação para assegurar o desempenho de gestão de riscos ou de funções de segurança da informação
- Educar os utilizadores de forma a satisfazer os objetivos do programa de segurança (que pode incluir normas, procedimentos e práticas impostas pelo setor de atividade, por parceiros de negócio ou por enquadramento legal)

Luís Borges Gouveia, lmbg@ufp.edu.pt

Aspetos da sensibilização para a segurança da informação

- Politicas de segurança da organização
- Programa de segurança da organização
- Requisitos de conformidade impostos pelos reguladores
- Engenharia social
- Continuidade de negócio
- Recuperação de desastres
- Gestão de emergências
- Resposta a incidentes de segurança
- Classificação de informação
- Manipulação e descrição de informação
- Segurança pessoal e de pessoas
- Segurança física
- Uso apropriado de recursos computacionais
- Uso adequado de credenciais de segurança
- Avaliação de risco
- Acidentes, erros e omissões

Métodos e atividades de sensibilização para a segurança da informação

- Cursos formais, presenciais ou em regime de *e-learning*
- Realizar a análise de unidades de negócio, no local
- Usar uma intranet para colocar avisos de segurança e manter uma área sobre o tema da segurança
- Descobrir os campeões para a segurança da informação, na organização
- Patrocinar um dia para a sensibilização da segurança da informação
- Patrocinar um evento sobre a segurança da informação, com um parceiro externo
- Criar peças de informação para os utilizadores, promovendo as boas práticas e bons exemplos, na segurança da informação
- Facilitar o acesso a materiais como vídeos, livros, sites Web e outros para referenciar o tema da segurança da informação

Certificação de segurança

- A certificação de segurança é a avaliação exaustiva dos controlos de segurança técnica, mas também dos aspetos associados com a gestão e operações nos sistemas de informação da organização
- Deve permitir a acreditação de segurança e determinar até que ponto, estes controlos estão implementados de forma correta, funcionam como pretendido e produzem os efeitos desejados para cumprir os requisitos de segurança do sistema
- Os resultados da certificação de segurança são utilizados para reavaliar e atualizar o plano do sistema de segurança, proporcionando a base de evidências para um auditor poder suportar a decisão de acreditação de segurança

A acreditação em segurança da informação

- Quando um sistema de informação é acreditado, por uma entidade certificada para o efeito, significa que os riscos da sua operação são aceites
- As implicações associadas com as operação, os ativos e as implicações com os indivíduos são levantados e explicitados
- O esforço de acreditação assegura que um sistema de informação é operado com uma revisão de gestão adequada e que existem os controlos de segurança de supervisão
  - A re acreditação pode ocorrer de forma periódica de acordo com as políticas de segurança em curso ou quando as condições de operação ou de mudança no ambiente, assim o exigirem
- Os objetivos dos guias de orientação são:
  - Possibilitar a avaliação dos controlos de segurança de forma mais consistente, comparável e repetível
  - Promover um melhor entendimento dos riscos de operação envolvidos num sistema de informação
  - Criação de um mecanismo mais completa, fiável e confiável para autorização e facilitação da tomada de decisão sobre a acreditação de sistemas complexos

Em Portugal, a credenciação em segurança da informação é responsabilidade do Gabinete Nacional de Segurança (GNS, *http://www.gns.gov.pt/)*

- Superintender tecnicamente nos procedimentos nas entidades, públicos ou privados, tendo em vista a garantia da proteção e salvaguarda da informação classificada no âmbito nacional e da representação do Estado Português no exterior
- Garantir o cumprimento das medidas de proteção da informação classificada
- Atribuir, controlar e revogar a credenciação de segurança de pessoas singulares ou coletivas, públicas ou privadas
- Determinar a fiscalização e a inspeção periódica de órgãos de segurança detentores de informação classificada sob responsabilidade portuguesa
- Autorizar a abertura e determinar o encerramento de órgãos de segurança detentores de informação classificada sob responsabilidade portuguesa
- Determinar a avaliação, a acreditação e a certificação de produtos e sistemas de comunicações, de informática e de tecnologias de informação
- Difundir orientações para a elaboração dos planos de emergência e de contingência destinados a precaver e ou evitar comprometimentos, quebras ou violações de segurança de informação classificada
- Determinar a abertura de inquéritos de segurança e proceder à respetiva instrução
- Emitir normas técnicas sobre os procedimentos a adotar pelos órgãos de segurança da informação classificada

Em Portugal, a credenciação em segurança da informação é responsabilidade do Gabinete Nacional de Segurança (GNS, *http://www.gns.gov.pt/)*

- Conferir certificados de habilitação exigidos por disposição legal ou regulamentar para requerer a credenciação de segurança, às pessoas que desempenhem funções em locais onde é administrada informação classificada
- Exercer as competências de credenciação de segurança, proceder ao registo e exercer as demais competências de autoridade credenciadora e de fiscalização das entidades certificadoras
- Atribuir credenciação de segurança nacional às empresas que pretendam exercer as atividades de comércio e indústria de bens e tecnologias militares
- Atribuir credenciação de segurança a entidades públicas e privadas para o exercício de atividades industriais, tecnológicas e de investigação
- Atribuir credenciação de segurança no âmbito do Sistema GALILEO e proceder à gestão das chaves da sua componente de segurança
- Determinar a realização de limpezas eletrónicas no âmbito de avaliação de ambientes de segurança nas componentes geral, local e eletrónica
- Representar Portugal nas reuniões que tratem da proteção e salvaguarda da informação classificada
- Propor a celebração e colaborar na elaboração dos Acordos Bilaterais de Segurança da informação classificada

Luís Borges Gouveia, lmbg@ufp.edu.pt

A credenciação de pessoal no contexto nacional

- Norma técnica A 01 (janeiro de 2013)
  - Da responsabilidade do Gabinete Nacional de Segurança
  - De acordo com a Lei 49/2009 de 5 de Agosto
  - A norma regula e enquadra o preenchimento da ficha individual para credenciação de pessoal *http://www.gns.gov.pt/media/1136/NTA01NovaVers%C3%A3oJan2013.pdf*
- Credenciação de Pessoas Singulares (privados), atuando como profissionais liberais ou por conta própria
  - Enquadra elementos civis, como os consultores, assessores, etc.
  - Considera um tempo limitado, normalmente um ano
  - Toma os mesmos procedimentos dos realizados para pessoas singulares
- Existem custos associados e taxas a pagar, para efeitos de acreditação e credenciação

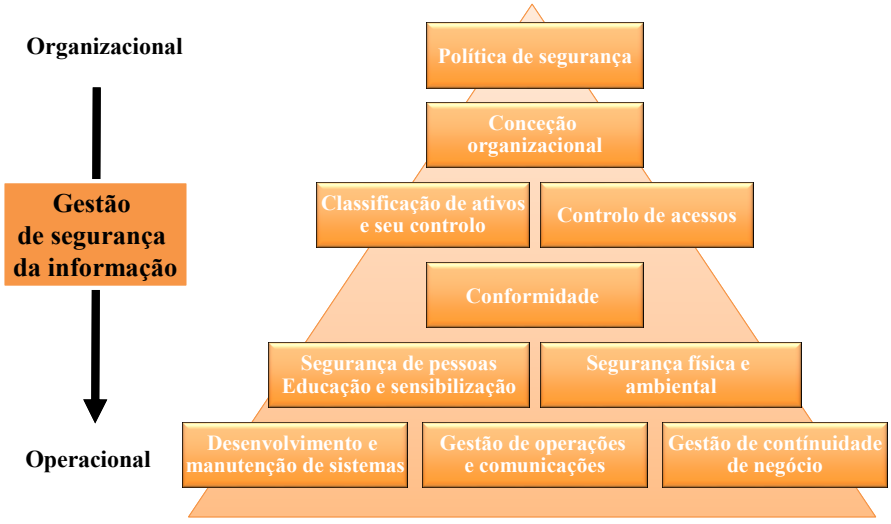
Se as pessoas são importantes, a sua literacia não é menos

Enquadrar a segurança da informação

PLANEAMENTO DE SEGURANÇA DA INFORMAÇÃO NA ORGANIZAÇÃO

Luís Borges Gouveia, lmbg@ufp.edu.pt

Hierarquia de atividades de gestão da segurança da informação



Luís Borges Gouveia, lmbg@ufp.edu.pt

Planeamento da segurança de informação

- O planeamento reduz a possibilidade de que a organização se torne reativa na abordagem das suas necessidades de segurança
- O planeamento de segurança envolve o desenvolvimento de políticas de segurança e a implementação de controlos de forma a prevenir riscos de segurança da informação de se tornarem realidade
- A avaliação de risco proporciona a base para a implementação de planos de segurança de modo a proteger os ativos contra as diferentes ameaças

Luís Borges Gouveia, lmbg@ufp.edu.pt

Hierarquia do planeamento de segurança de informação

- Planeamento estratégico (3 a 5 anos)
  - O planeamento estratégico está alinhado com a estratégia de negócio e o plano estratégico dos sistemas de informação
  - Proporcionam a visão para os projetos atingirem os objetivos de negócio.
  - Estes planos devem ser revistos anualmente ou sempre que uma grande mudança ocorra
- Planeamento tático (6 a 18 meses)
  - Os planos táticos proporcionam as iniciativas mais alargadas para suporte e alcance dos objetivos especificados nos planos estratégicos
- Planeamento operacional e de projetos (dia, semana ou mês)
  - Planeamento específico com metas a atingir, com datas e resultados concretos que permitam a comunicação e seguimento que assegura o sucesso de projetos individuais

Luís Borges Gouveia, lmbg@ufp.edu.pt

Tipos de planeamento de segurança de informação

- Planeamento proativo
  - Desenvolver políticas e controlos de segurança
  - Implementar ferramentas e técnicas para ajuda em segurança
    - Proteger acesso, proteger dados e proteger código
    - Técnicas de segurança de redes (*firewall*, VPN, …)
    - Ferramentas de deteção (IDS, …)
  - Implementar tecnologias para garantir o funcionamento do Sistema em caso de falha
- Planeamento reativo
  - Desenvolver um plano de contingência

Exemplos de planos de segurança de informação

- Plano de segurança de informação da *Michigan Technological University*: *http://www.security.mtu.edu/policies-procedures/information-security-plan.pdf*
- Um modelo completo formato MS Word para a criação de um plano de segurança:
  - *Federal Deposit Insurance Corporation* *https://www.fdic.gov/buying/goods/.../ITSecurityPlanTemplate.doc*

Estratégia de segurança: um método para definir políticas e controlos de segurança

- Prever ataque e avaliar o risco
  - Para cada tipo de ameaça
    - Para cada tipo de método de ataque
      - Estratégia proactiva
        - » Prever os possíveis danos
        - » Terminar as vulnerabilidades
        - » Minimizar as vulnerabilidades
          - Implementar um plano para desenvolver as políticas e controlos de segurança
        - » Realizar planos de contingência
      - Estratégia reativa
        - » Avaliar danos
        - » Determinar a causa dos dados
        - » Reparar danos
          - Implementar plano e desenvolver políticas e controlos de segurança
        - » Documentar e aprender
        - » Implementar o plano de contingência
- Rever o resultado e simular
- Rever a eficácia da política
- Ajustar a política em resultado da prática

As responsabilidades do CISO
Chief Information Security Officer

- Comunicar os riscos à gestão executiva
- Orçamentar as atividades de segurança da informação
- Assegurar o desenvolvimento de políticas, procedimentos, linhas de ação, normas e práticas
- Desenvolver e conduzir um programas de sensibilização para a segurança da informação
- Entender os objetivos de negócio
- Manter a conciência para as ameaças e vulnerabilidades emergentes
- Avaliação de incidentes de segurança e da resposta a estes
- Desenvolver um programa de aplicação de segurança da informação
- Estabelecer métricas de segurança
- Participar em reuniões de gestão
- Assegurar a conformidade com as regulamentações legais
- Apoiar auditorias internas e externas
- Estar atualizado sobre as tecnologias emergentes

Boas práticas para a segurança na organização

- Rotação de trabalho
  - Reduz o risco de arranjo ou combinação de atividades entre indivíduos. Desta forma, as rotinas e hábitos personalizados são reduzidos
- Separação de tarefas
  - Um indivíduo não deve ter a capacidade para executar todas as etapas de um processo específico e o controlo total sobre um processo
- Menor privilégio (necessário conhecer)
  - Conceder aos utilizadores apenas os acessos que são necessários para realizar as suas funções de trabalho
- Férias obrigatórias
  - Exigir o gozo de férias de forma obrigatória pelos trabalhadores, num período consecutivo de dias especificado
- Criticidade da posição de trabalho
  - O acesso e os direitos de um indivíduo para um dado contexto na organização, deve ser avaliado para determinar a criticidade da posição que ocupa

Separação de tarefas

- O mesmo indivíduo não deve ser o mesmo que realiza as seguintes funções:
  - Administração de sistemas
  - Gestão da rede
  - Entrada de dados
  - Operações de computador
  - Gestão da segurança
  - Desenvolvimento e manutenção de sistemas
  - Auditoria de segurança
  - Gestão de sistemas de informação
  - Gestão da mudança

Segurança e pessoal: práticas de contratação

- Gerir pessoas é essencial para a segurança da informação
- A contratação de recursos humanos faz parte das preocupações com a segurança e implica desde logo que a proteção de dados e informação da organização comece nesta atividade, obrigando à atenção dos seguintes aspetos:
  - Desenvolver descrições e o perfil de emprego
  - Desenvolver acordos de confidencialidade
  - Contatar as referências fornecidas (e verificar as referências)
  - Verificar e investigar os antecedentes do indivíduo
  - Supervisionamento contínuo e avaliações de desempenho periódicas
  - Determinar políticas de acesso a informação para fornecedores, consultores e pessoal temporário
  - A terminação de vínculos laborais também necessita de diferentes níveis de preocupação

Verificar e investigar os antecedentes do indivíduo

- Os antecedentes e história profissional pode proporcionar informação relevante do ponto de vista da segurança:
  - Falhas temporais entre empregos
  - Não especificação dos cargos realizados
  - As obrigações associados com cada emprego
  - Salário
  - Razões para sair do emprego
  - Validação e estado da certificação profissional
  - Verificação das habilitações e graus obtidos
  - Reputação e histórica ou sequência de trabalhos
  - Registos da carta de condução
  - Registo criminal
  - Referências pessoais
  - Verificação dos dados pessoais e de identidade

Tipos específicos de verificação de antecedentes

- Indivíduos envolvidos em tecnologia
- Indivíduos com acesso a informação sensível ou confidencial
- Trabalhadores com acesso a dados proprietários ou competitivos para a organização
- Posições que trabalham com a contabilidade, recebimentos ou pagamentos
- Posições que trabalham diretamente com o público
- Trabalhadores associados com a industria dos cuidados de saúde ou organizações que lidam com informação financeira
- Posições que envolvam a condução de veículos de transporte
- Trabalhadores que entrem em contato com criança

Atividades de planeamento na organização, associadas com a segurança da informação

- Desenvolver um plano de segurança da informação
- Rever e propor uma estrutura para a segurança na organização
- Desenvolver um plano de aquisição de segurança, incluindo a descrição de trabalho para as posições de segurança
- Desenvolver um programa de verificação continua da segurança da informação
- Desenvolver um programa de consciencialização da segurança da informação
- Desenvolver um plano de formação e treino em segurança de informação

Um plano não é um contrato…

Enquadrar a segurança da informação

QUESTÕES ÉTICAS

Enquanto responsável pela segurança da informação numa organização

- É necessário entender o âmbito das responsabilidades legais e éticas da organização
- De forma a minimizar responsabilidades e a reduzir riscos, quem pratica segurança da informação deve:
  - Entender o ambiente jurídico em vigor
  - Manter-se atualizado com as leis e os regulamentos
  - Prestar atenção para novos problemas que emergem

Lei e ética em segurança da informação

- **Lei**: as regras que regulam ou proíbem certos comportamentos na sociedade
- **Ética**: define os comportamentos aceitáveis na sociedade
- **Costumes culturais**: atitudes ou costumes fixos de um determinado grupo
  - A ética é baseada nestes e por razões culturais, associada a uma **moral** (moralidade)
- As leis levam a sanções emanadas pela autoridade de governo e do Estado; a ética, não

Responsabilidade organizacional e necessidade de aconselhamento

- Responsabilidade: obrigação legal de uma entidade que se estende para além do direito penal ou contrato legal; inclui obrigação legal de fazer a restituição do valor de perda potencial
- Restituição: para compensar erros cometidos por uma organização ou dos seus funcionários
- Cuidado devido: garantindo que os funcionários sabem o que constitui um comportamento aceitável e sabem as consequências de ações ilegais ou antiéticas
- Diligência de zelo: realizar um esforço válido para proteger os outros; manter continuamente esse nível de esforço
- Jurisdição: o direito do tribunal para ouvir um caso se o erro foi cometido no seu território ou envolver os seus cidadãos
- Braço longo da jurisdição: direito de qualquer tribunal para impor a sua autoridade sobre um indivíduo ou organização, se poder ser estabelecida a sua jurisdição

Políticas versus leis

- **Políticas**: corpo de expetativas que descreve comportamentos aceitáveis e não aceitáveis no local de trabalho ou com a forma como lida com a informação da organização
- Politicas funcionam como leis, dentro de uma organização
  - Devem ser desenvolvidas de forma cuidadosa de modo a assegurar que são completas, apropriadas e aplicadas de forma justa a todos
- Diferença entre política e lei: ignorância de uma política é uma defesa aceitável (da lei, não)
- Critérios para obrigar a uma política:
  - disseminação (distribuição)
  - revisão (leitura)
  - compreensão (entendimento)
  - conformidade (aceitação)
  - aplicação uniforme (igualdade de tratamento)

Ética e segurança da informação

Os 10 mandamentos de ética de computador (*Computer Ethics Institute*)

1. Não usar um computador para causar mal a outra pessoa
2. Não interferir com o trabalho de computador de outra pessoa
3. Não espreitar ou explorar os ficheiros de computador de outra pessoa
4. Não usar um computador para roubar
5. Não usar um computador para levantar falsas suspeitas
6. Não copiar ou utilizar software proprietário que não tenha sido adquirido
7. Não utilizar recursos computacionais de outras pessoas sem a sua autorização ou sem a devida compensação
8. Não ficar com os resultados do trabalho intelectual de outra pessoa
9. Deve pensar nas consequências sociais dos programas que desenvolve e dos sistemas que concebe
10. Deve usar sempre o computador de modo a assegurar a consideração e o respeito pelos outros

Ética e educação

- Um dos fatores preponderantes no nivelamento das perceções éticas no contexto de uma pequena população é a educação
- Os trabalhadores de uma empresa devem ser treinados em comportamentos esperados de um perfil ético, especialmente nas áreas de segurança da informação
- Uma formação ética adequada é vital para a criação de um utilizador do sistema, informado, bem preparado e de baixo risco

Dissuasão de comportamento ilegal e antiético

- Três das causas gerais para o comportamento ilegal e antiético são:
  - Ignorância
  - Acidente
  - Intenção
- Dissuasão: o melhor método para prevenir uma atividade ilegal ou antiética (por exemplo: leis, políticas e controlos técnicos)
- Leis e políticas apenas resultam, caso estejam presentes três condições:
  - Medo da pena
  - Probabilidade de ser apanhado
  - Probabilidade da pena ser executada

Códigos de ética de organizações profissionais

É responsabilidade dos profissionais de segurança agirem de forma ética e de acordo com as políticas do empregador, da organização profissional e das leis da sociedade

- *Association of Computing Machinery* (ACM)
  - É a associação mais antiga de informáticos (1947) e o seu código de ética possui referências à proteção de informação, da confidencialidade e da privacidade assim como o respeito pela propriedade intelectual e salvaguarda de dados e informação de terceiros
- *International Information Systems Security Certification Consortium*, $(ISC)^2$
  - Organização não lucrativa focada no desenvolvimento e implementação de certificações e credenciações em segurança da informação. Possui um código de ética concebido para profissionais com certificações ISC2
- *Information Systems Audit and Control Association* (ISACA)
  - Organização profissional focada em auditorias de controlo e segurança. Concentra-se em fornecer controlos de prática e normas para TIC. Possui um código de ética para os seus profissionais
- *Information Systems Security Association* (ISSA)
  - Associação não lucrativa de profissionais de segurança da informação, focada na partilha de boas práticas e partilha de conhecimento. Possui um código de ética semelhante ao ISC2 , ISACA e ACM

Diferença entre ética e lei

Ética	Lei
Um guia de orientação para as utilizadores de computadores	Uma regra para controlar utilizadores de computador
Os utilizadores de computador são livres de seguir ou ignorar um código de ética	Os utilizadores de computador devem seguir as leis e os regulamentos
Universal, pode ser aplicado em qualquer lugar, em todo o mundo	Depende do país em que o crime é cometido
Para produzir utilizadores de computador éticos	Prevenir o mau uso de computadores
Não seguir princípios éticos é chamado imoral	Não obedecer a leis é chamado crime

Luís Borges Gouveia, lmbg@ufp.edu.pt

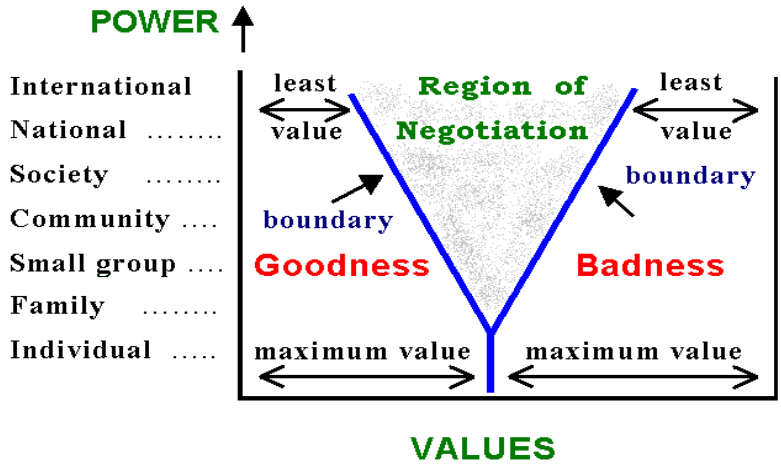
Definição de conceitos

Conceito	Descrição
Ética de computadores	É um sistema de normas morais ou valores moais utilizado como guia de orientação para os utilizadores de computadores
Código de ética	É um guia de orientação para as tecnologias de informação e comunicação que ajuda a determinar se uma ação de computador específica é ética ou antiética
Propriedade intelectual	É o trabalho criado por inventores, autores ou artistas
Privacidade	Refere o direito de indivíduos e organizações a negar ou restringir a recolha ou uso de informação dos próprios
Crime informático	É um qualquer ato ilegal que envolva computadores
Ciberlei	É uma qualquer lei relacionada com a proteção da Internet ou outra tecnologia de comunicação em linha

Luís Borges Gouveia, lmbg@ufp.edu.pt

Gráfico de negociação

Ética e valores de sobrevivência



http://website.lineone.net/~ian_heath2/4f-personal%20evolution.htm

Luís Borges Gouveia, lmbg@ufp.edu.pt

Como lidar com os riscos da Internet em segurança da informação

POLÍTICAS DE INFORMAÇÃO

Luís Borges Gouveia, lmbg@ufp.edu.pt

Segurança da informação, também passa pela segurança da Internet

"Os noticiários estão repletos de relatórios sobre segurança na Internet, que são muito críticos e alertam para os perigos e riscos dos negócios digitais (no entanto, incontornáveis, no contexto atual)

A fraude baseada na rede está a crescer de forma dramatica e torna a segurança na Internet um assunto crítico para o negócio e não apenas uma questão técnica"

Segurança da informação e segurança na Internet

- Principais razões de ataque
  - Erro humano
  - Falta de procedimentos adequados
  - Software mal configurado
- Discussão…
  - São vulnerabilidades?
  - São ameaças?
  - São riscos?

Requisitos importantes

- Confidencialidade
  - Necessário para controlar quem acede e usa a informação e para a ocultação de informação sensível
- Integridade
  - Assegurar que a informação e programas são lterados somente de maneira controlada e autorizada, e que os dados apresentados são genuínos e não foram adulterados, qualquer que seja a operação em causa
- Disponibilidade
  - Garantir que os utilizadores autorizados continuam a ter acesso a informação e recursos, sempre que o necessitem

- Legitimidade
  - Assegurar que os recursos não podem ser usados por pessoas não autorizadas ou de um modo não autorizado
- Não repúdio
  - Assegurar os mecanismos que garantam que uma pessoa ou empresa não possa negar uma transação que realizou ou uma informação que proveu

Luís Borges Gouveia, lmbg@ufp.edu.pt

Política de informação: motivação

"Todo a empresa precisa de desenvolver uma política de informação que assegure que os processos estão disponíveis quando algo acontecer"

"A segurança não pode ser medida pelo retorno sobre o investimento"

Luís Borges Gouveia, lmbg@ufp.edu.pt

Política de informação

- Fazer uma lista de todos os recursos que precisam de ser protegidos
- Definir quem tem acesso físico ao hardware e acesso lógico ao software
- Catalogar as ameaças para cada um dos recursos
- Uma vez catalogadas as ameaças, uma análise de risco deve ser realizada, explicitando a percentagem de possibilidade para cada ameaça
- Avaliar quais ameaças que podem ser ignoradas ou consideradas menos importantes e as que precisam ser consideradas críticas
- Devem ser realizadas avaliações regulares e atualizações no caso de novas ameaças ou de uma falha na segurança (incidente)

Ameaças na Internet

- Perda de integridade de dados
  - A informação é criada, modificada ou apagada por um intruso
- Perda de privacidade de dados
  - A informação é disponibilizada para pessoas não autorizadas
- Perda de serviço
  - Um serviço pára devido à ação de um um elemento exterior
- Perda de controlo
  - Os serviços são usados por pessoas autorizadas de um modo não controlado

Formas de atacar um sistema

- Capturar e seguir a comunicação entre duas partes
- Roubo do software e/ou hardware
- Interceptar e monitorizar dispositivos
- Utilização de “Cavalos de Tróia”
- Falsificação (*spoofing*) de IPs
- Captura de recursos de media descartados pela empresa (disquetes, cd-rom, dvd, canetas usb, etc.)
- Suborno do pessoal de segurança do alvo
- Intrusão física
- Divulgar informação sobre a rede interna

Luís Borges Gouveia, lmbg@ufp.edu.pt

Engenharia social

- Explorar os hábitos das pessoas, de forma a que elas não notem que alguém roubou ou deu informações falsas
- Concentra-se no elo mais fraco da segurança da Internet – o ser humano
- A abertura ao exterior e os eventos sociais facilitam a entrada em qualquer sistema de computador, porque são independentes de plataformas de sistema de ataque, sistema operativo e software de aplicação
- A dimensão social permite a interação com trabalhadores e interesses diversos que normalmente de forma indireta, permitem a qualquer pessoa alguma forma de contato com as pessoas envolvidas com a segurança da rede da empresa – um potencial risco de segurança

Luís Borges Gouveia, lmbg@ufp.edu.pt

Vulnerabilidades que exploram a Engenharia Social (ES)

- Os recursos humanos, em especial:
  - Recepcionistas, telefonistas, motoristas e empregadas de limpeza
  - Secretárias e trabalhadores de suporte a atividades especializadas
  - Estagiários, trabalhadores temporários e seguranças
- "Lixo" da empresa:
  - Existem destruidores de papel?
  - Existem políticas de papel reciclado?
- Disquetes, CD-ROMs, DVDs, canetas USB e discos rígidos, etc.
  - São deixados em livre acesso?
  - Podem ser usados em qualquer equipamento?
- Perguntas directas
- Obtenção de informação e pressão social
- A natureza humana, em especial a curiosidade
  - O correio eletrónico é o meio mais comum para a exploração da ES

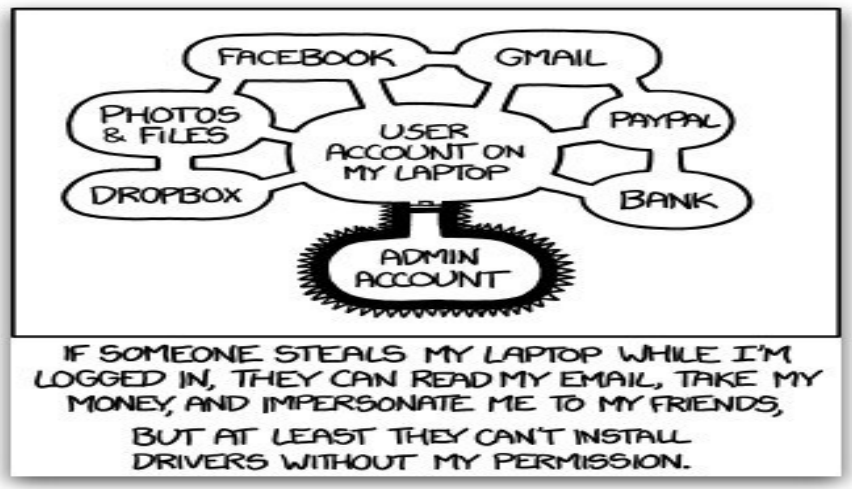
Formação e treino

"A fim de tornar a engenharia social menos provável de ser explorada, é necessário educar todos na empresa. Todo o trabalhador/colaborador precisa de entender a importância da segurança e quais os métodos utilizados para eliminar as barreiras e quebrar a segurança"

Segurança através da obscuridade

"*Ainda é uma estratégia muito comum utilizada pelas empresas, que tentam evitar lidar frontalmente com falhas de segurança. Ignorando os aspectos de segurança, os fornecedores de software esperam que ninguém documente as falhas e encontre meios de as explorar*"

A segurança começa nas pessoas
(cultura de segurança)



CUSTO E RETORNO NA SEGURANÇA DA INFORMAÇÃO

Luís Borges Gouveia, lmbg@ufp.edu.pt

Avaliar os custos de segurança

- Convencer a direção que o investimento na segurança da informação ou na continuidade de negócio faz sentido, é dificil e exige uma abordagem adequada:
  - Tradicionalmente, para os gestores, implica que os retornos do investimento sejam maiores que os custos do investimento
  - É importante referir que esta visão pode ser uma simplificação excessive, pois tratando-se de atividades críticas, é por vezes necessário assegurar a sua total segurança, sendo a contabilização de perda não apenas económica, mas de prestígio ou até com implicações extremas
- Deste modo, o desafio é saber como calcular o retorno de investimento em segurança da informação
  - Mesmo calculando o custo, não existe um retorno a ser realizado
  - Podem existir poupanças de custos mais ou menos óbvias
  - Mas o custo de segurança é dificil de calcular, caso não existam incidentes e esses são precisamente evitados pelo investimento

Luís Borges Gouveia, lmbg@ufp.edu.pt

Avaliar o custo de segurança da informação

- Uma abordagem possível é estimar os benefícios financeiros (poupança de custos) da segurança da informação
  - Estimar o potencial dano que um incidente possa causar
  - Estimar a possibilidade de ocorrência de um incidente
  - Avaliar a frequência de um potencial incidente após implementação de medidas de segurança
  - Estimar o custo das medidas de segurança
  - Calcular o valor final de retorno do investimento em segurança

Estimar o potencial dano que um incidente possa causar

Primeiro passo

- Estimar o potencial dano que um incidente possa causar – *Single Lost Expectancy* (SLE)
- Cálculo do SLE:
  - O contexto do potencial incidente (quais os departamentos, funções, unidades de negócio e processos que são afetados)
  - O custo de aquisição de equipamento, bens e materiais que são danificados com o incidente
  - Trabalhadores (o custo dos recursos humanos envolvidos na resolução do incidente)
  - Penalizações legais e/ou contratuais (resultado de não conformidade ou infração legal e com eventuais quebras de contrato)
  - Perda de receitas (quer de clientes existentes, quer de potenciais clientes)

Estimar a possibilidade de ocorrência de um incidente

Segundo passo

- Para estimar a possibilidade de ocorrência, consideram-se as ameaças e as vulnerabilidades, assim como as medidas de segurança existentes
  - Um dos melhores modos de avaliar a frequência com que um incidente pode ocorrer (por exemplo, uma vez por mês; de dois em dois anos; ou a cada 200 anos)
- Multiplicar o valor obtido no primeiro passo (*Single Lost Expectancy*) pela possibilidade de ocorrência, obtendo a *Annualized Lost Expectancy* (ALE)
  - Este valor pode ser considerado o custo anual do risco. Assim, o custo anual de um terramoto custaria 7,5 milhões de euros, se o SLE fosse de 1500 milhões de euros e a possibilidade de uma ocorrência, fosse uma a cada 200 anos

Avaliar a frequência de um potencial incidente após implementação de medidas de segurança

Terceiro passo

- Avaliar a frequência do potencial incidente depois de implementadas as medidas de segurança
  - No exemplo do terramoto, a frequência será a mesma
  - No entanto, se for implementado software anti-vírus mais eficaz, a possibilidade de ataque de software malicioso será menor
  - Existem assim casos que podem anular o risco ou apenas mitigar o mesmo (embora existam casos em que o rsico não pode ser anulado)

Estimar o custo das medidas de segurança

Quarto passo

- Qual o custo das medidas de segurança, tendo em conta diversos fatores:
  - Valor de compra: custo de hardware, software, serviços de implementação, etc.
  - Valor residual da medida de segurança: é o valor após cessar o seu uso
  - Custos externos de manutenção: serviços, reparação, etc.
  - Custos internos de manutenção: no essencial, recursos humanos e consumíveis

Calcular o valor final de retorno do investimento em segurança

Quinto passo

- Quando forem recolhidos os dados dos quatro passos anteriores, obtêm-se o valor de retorno do investimento em segurança (*Return on Security Investment*), que pode ser positivo ou não
  - A diminuição do risco tem de ser maior que o total de custos das medidas de segurança
  - É recomendável realizar os cálculos tendo como base o período de um ano. Tal significa que as perdas esperadas anuais (*Annualized Lost Expectancy*) tem de produzir um valor que seja maior que os custos anuais das medidas de segurança (garantindo um custo económico de segurança que seja realizável para o context em análise)

Retorno de Investimento em Segurança (*Return on Security Investment,* ROSI)

- É desafiante provar que o investimento em segurança tem retorno
- A definição do retorno de investimento em segurança pode ser dados pela fórmula:
  - ROSI = ganho com a mitigação do risco – custo do controlo
- Deste modo, um investimento em segurança é considerado com retorno, se o efeito da mitigação do risco é maior que os custos esperados
- Uma análise do ROSI tem os seguintes passos:
  - *Passo 1*: calcular o custo de um incidente, considerando todos os custos relevantes que ocorrem e a probabilidade de corrência desse incidente
  - *Passo 2*: calcular o custo das medidas ou controlos de segurança e o nível de risco que é mitigado do incidente
  - *Passo 3*: o resultado final é a verificação se existe um ganho efetivo (o risco diminui) é maior que a necessidade de investimento (medidas ou controlos de segurança)

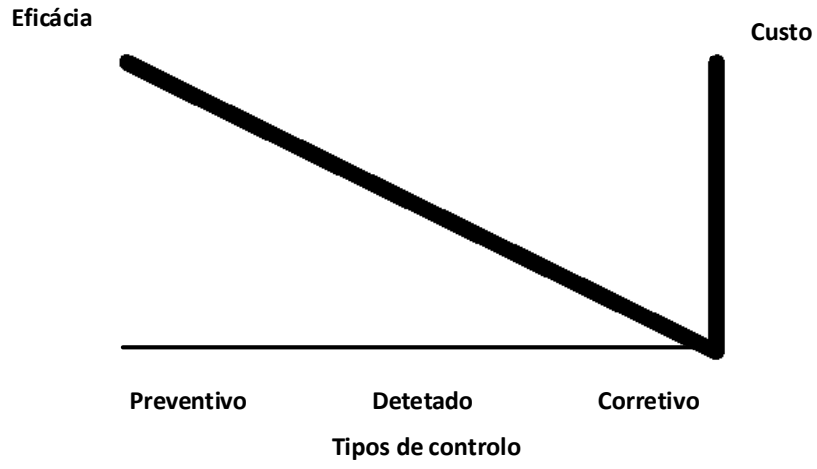
Valor atual líquido (Net present value, NPV) para a segurança da informação

- $NPV = I_0 + \sum_{t=1}^{T} \frac{\Delta E(L_t) + \Delta OCC_t - C_t}{(1 + i_{calc})^t}$

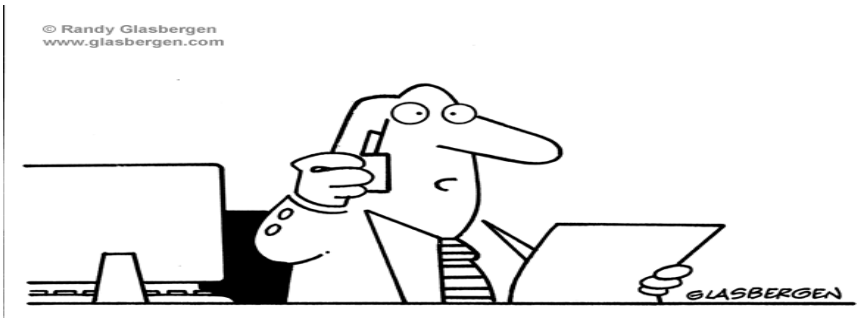
  - I_0: investimento inicial para a medida de segurança
  - $\Delta E(L_t)$: Redução na perda esperada em t
  - ΔOCC_t: Redução em custos de oportunidade em t
  - C_t: custo da medida de segurança em t
  - i_{calc}: taxa de desconto

http://www.kannan-subbiah.com/2014/11/information-security-cost-analysis.html#.VkuQ4XbhBpg

A fase de intervenção é também importante
As dimensões de controlo, da eficácia e do custo



Existe igualmente o custo do (des)conhecimento



"I sent my bank details and Social Security number in an e-mail, but I put 'PRIVATE FINANCIAL INFO' in the subject line so it should be safe."

2: **Proteção de dados individuais**
- 2.1. Conceitos associados
- 2.2. Desafios e mecanismos de proteção
- 2.3. A vertente empresarial e a informação sensível
- 2.4. A vertente individual
- 2.5. Legislação e enquadramento

SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS INDIVIDUAIS

Luís Borges Gouveia, lmbg@ufp.edu.pt

"Existem uma tendência crescente para a passagem da proteção de equipamentos para a proteção de dados"

"Os dados são o novo capital"

"Parte da capacidade de inteligência dos sistemas é definida com base na exploração e análise de dados e informação: da inteligência de negócios à ciência de dados, emerge uma crescente sofisticação e potencial do uso de dados para criar valor"

Luís Borges Gouveia, lmbg@ufp.edu.pt

A noção de proteção de dados

- A proteção de dados significa a proteção legal da privacidade de um indivíduo através da regulação do processamento dos seus dados pessoais e
- Da salvaguarda de determinados direitos associados com os seus dados
- Surgiu na Europa como uma resposta aos perigos do processamento eletrónico de dados que se desenvolveu com o surgimento das tecnologias de informação, a partir da década de 1970

O que é a privacidade?

- Uma afirmação, um atributo ou um direito que um indivíduo possui para determinar qual a informação sobre si próprio que pode ser comunicada aos outros
  - Uma medida de controlo que um indivíduo possui sobre a sua informação pessoal (privacidade de informação, implica privacidade de dados)
- Intimidade da identidade pessoal ou a quem tem acesso sensorial ao indivíduo
- Um estado ou condição de acesso limitado a uma pessoa, à informação sobre a pessoa, ou elementos intimos da identidade pessoal
- O direito à privacidade é o direito de ser deixado sozinho e o direito ao esquecimento

Definição e dimensões da privacidade

- Privacidade
  - O direito dos indivíduos, grupos e instituições de determinar por si próprios, quando, como e até que extensão, informação sobre si é comunicada a outros
- Três dimensões da privacidade:
  - **Privacidade pessoal**: protege a pessoa contra interferencia de terceiros e também de informação que viole o seu senso moral
  - **Privacidade territorial**: protege uma área física em torno de uma pessoa que não pode ser violada, sem o consentimento dessa pessoa
  - **Privacidade informacional**: lida com a recolha, compilação e disseminação seletiva de informação

Princípios de privacidade

- Princípios básicos de privacidade
  - Legalidade e equidade
  - Necessidade de recolha de dados e de processamento
  - Especificação de propósito e da relação com o propósito
  - Tansparência (direito de acesso e correção, eliminação ou bloqueio de dados incorretos ou ilegais)
  - Supervisão (controlo por entidades independentes que constituam autoridades de proteção de dados e com sanções aplicáveis, se necessário)
  - Salvaguardas técnicas e organizacionais adequadas

Mecanismos de proteção

- A proteção de privacidade pode ser implementada por:
  - Leis de privacidade e de proteção de dados promovidas pelos governos
  - Auto regulação para práticas de informação justas, promovidas por códigos de conduta associados com áreas de negócio específicas
  - Tecnologias de suporte à privacidade, adoptadas por indivíduos e organizações
  - Educação para a privacidade de consumidores e profissionais de tecnologias de informação e comunicação

Proteção de dados e segurança de dados

- Proteção de dados
  - Uma ferramenta para a proteção da privacidade, direcionada para os dados pessoais
- A proteção de dados é quase sempre, uma proteção legal
- Segurança de dados
  - A proteção da integridade e confidencialidade de dados, independentemente do conteúdo de informação e da qualificação legal desses dados
- A segurança de dados é objeto de medidas legais, técnicas e organizacionais

Proteção de dados e segurança de dados

- Complexa rede de ligações entre proteção de dados e segurança de dados
  - A maior parte das leis de proteção de dados possuem regras sobre segurança de dados
  - Num ambiente de rede aberta, as ferramentas de segurança de dados devem ser, pelo menos, tão eficazes para proteção como o especificado pelas leis (tecnologias PET – *privacy-enhanced technologies*)
  - Ferramentas de segurança de dados podem ser objeto de regulação legal (com exigências de requisitos mínimos…)

O que são dados pessoais

- Dados pessoais compreendem qualquer informação relacionada com uma pessoa (sujeito de dados)
- Uma pessoa é um indivíduo que possa ser identificado de forma direta ou indireta, por via de uma referência como um número de identificação ou por um ou mais fatores específicos da sua identidade física, psicológica, mental, económica, cultural ou social
(*Diretiva 96/46/EC*)

Privacidade versus segurança

http://www.claybennett.com/pages/security_fence.html

Iniciativas iniciais e o exemplo Inglês

PROTEÇÃO DE DADOS, MAU USO DA INFORMAÇÃO E PROPRIEDADE

Dados e informação pessoal

- Várias questões podem ser colocadas
  - Quem pode aceder a informação pessoal?
  - Até que ponto é que essa informação é correta?
  - Essa informação pode ser copiada?
  - É possível armazenar essa informação sem o conhecimento do indivíduo e a sua permissão?
  - É realizado um registo de mudanças e acessos realizados a essa informação?

Data Protection Act (1998)

O que é e porque foi criada?

- A lei de proteção de dados Inglesa enuncia as regras de como os dados pessoais podem ser utilizados
- Foi criada para proteger inívíduos do mau uso dos seus dados pessoais
- Governa igualmente a coleção e processamento de dados pelas organizações e o direito dos indivívduos, do acesso aos seus dados, se o pretenderem
- Texto integral disponível em *http://www.legislation.gov.uk/ukpga/1998/29/contents*

Data Protection Act (1998)

Quais são os seus oito (8) princípios?

1. Os dados devem ser mantidos seguros
2. Os dados armazenados devem ser relevantes
3. Os dados armazenados devem ser mantidos apenas durante o tempo necessário
4. Os dados armazenados devem ser mantidos de forma precisa e atualizada
5. Os dados devem ser obtidos e processados de forma legal
6. Os dados devem ser processados no quadro dos direitos dos temas a que a recolha dos dados está associada
7. Os dados devem ser obtidos e especificados com finalidades legais
8. Os dados não devem ser transferidos para países se, leis de proteção de dados adequadas

Luís Borges Gouveia, lmbg@ufp.edu.pt

Data Protection Act (1998)

Quais os direitos que o indivíduo possui sobre os seus dados?

- Tomar conhecimento dos dados guardados sobre o indivíduo
- O direito de modificar os dados errados
- O direito de prevenir que os dados pessoais sejam utilizados, se causarem danos
- O direito de retirar os dados se estes forem usados na tentative de vender algo
- Recorrer à lei para ganhar uma compensação (ressarcimento)

Luís Borges Gouveia, lmbg@ufp.edu.pt

Data Protection Act (1998)

O que são os conceitos implicados na lei?

- *Information Commissioner* (oficial de lei)
  - Pessoa que possui o poder de fazer cumprir a lei
- *Data Controller* (controlador dos dados)
  - Pessoa ou organização que recolhe e armazena os dados sobre as pessoas
- *Data Subject* (sujeito dos dados)
  - Pessoa que possui os seus dados armazenados, fora do seu controlo direto

Data Protection Act (1998)

Existem isenções à lei de proteção de dados?

- Quaisquer dados mantidos por razões de segurança nacional
  - A exemplo dos serviços secretos Ingleses (MI5)
- A polícia pode aceder a informação pessoal em contexto de investigação criminal
- Os impostos podem aceder a informação pessoal para cruzamento de dados
- Quaisquer dados mantidos para finalidade doméstica, como listas de aniversário, listas de endereços e contatos pessoais

Tipos de dados

- Existem dois tipos distintos de dados pessoais
  - Dados pessoais
  - Dados pessoais sensíveis
  - Se alguém acede a estes dados sem obter permissão está a realizar um acesso não autorizado

Direitos do sujeito de dados

1. Direito de acesso
2. Direito de correção
3. Direito de prevenir impacto negativo
4. Direito de prevenir uso para marketing direto
5. Direito de prevenir decisões automáticas
6. Direito de queixa ao oficial de lei
7. Direito de compensação

Cuidados a ter

- Não deixar informação de pessoas em local visível (como uma secretária)
- Fechar os cacifos e os armários do escritório
- Não deixar os dados visíveis no ecran (usar um protetor de ecran – *screensaver*)
- Não deixar o computador ligado ou sozinho
- Não escolher uma senha de entrada que seja fácil de adivinhar ou descobrir
- Não dar a senha de entrada a ninguém, nunca
- Nunca enviar nada por faz ou por correio eletrónico que não colocaria num postal
- Não forneça informação pessoal sem o consentimento do sujeito de dados ou verificar o pedido (para as isenções à lei)
- Os media sociais também estão sujeito à lei de proteção de dados
- Pensar antes de atualizar o estado em redes sociais (ex. Facebook, Twitter, etc.)
- Lembrar que a Internet não esquece…

Computer Misuse Act (1990)

O que é e porque foi criada?

- O *Computer Misuse Act* (1990) foi desenvolvida para lidar com os problemas do mau uso de computadores, nomeadamente os *hackers* e os vírus
  - *Hacker*: utilizador não autorizado que tenta ou consegue ganhar acesso a um computador ou sistema de informação
  - Vírus: um programa escrito para causar transtorno ou danificar um sistema de computador

Computer Misuse Act (1990)

Quais são os três princípios da lei?

- É ilegal aceder a dados não autorizados
  - Exemplo: *hacking*
- É ilegal o acesso a dados não autorizados e pretender repetir ou efetuar ganhos com eles
  - Exemplo: chantagem ou fraude
- É ilegal o acesso a dados não autorizados e alterar os mesmos
  - Exemplo: plantar vírus ou apagar ficheiros

Copyright, Design and Patents Act (1988)

Lei Inglesa de propriedade intelectual

- Introduzida para proteger as pessoas que criaram pelas originais de trabalho
  - Livros, música, filmes, jogos, aplicações
- Dois objetivos principais da lei
  - Assegurar que as pessoas sejam recompensadas pelos seus esforços
  - Proporcionar proteção para o detentor de direitos de cópia (*copyright*) se alguém tentar roubar o seu trabalho

Copyright, Design and Patents Act (1988)

Lei Inglesa de propriedade intelectual

- A lei protege um leque alargado de trabalhos
  - Desde textos até aos trabalhos baseados em computador
- A lista de trabalhos inclui (alguns deles posteriores a 1988):
  - Copiar Software
  - Copiar ou descarregar música
  - Copiar imagens ou fotografias da Web
  - Copiar texto de páginas Web

Site da Legislação Inglesa para consulta pública

http://www.legislation.gov.uk/ukpga/1998/29/contents

Enquadramento e contexto legal em Portugal

PROTEÇÃO DE DADOS

Luís Borges Gouveia, lmbg@ufp.edu.pt

Proteção de dados

- Um direito fundamental
  - Na europa
  - Linhas Directrizes da OCDE (1973)
  - Convenção 108 do Conselho da Europa (1981)
  - Directiva 95/46/CE
  - Carta dos Direitos Fundamentais da União Europeia
  - Tratado de Lisboa
  - Em Portugal: 1ª Constituição com norma expressa (1976)

Luís Borges Gouveia, lmbg@ufp.edu.pt

Diplomas legais

Hierarquização das leis em função da sua importância/dignidade

- Primeiro: **Lei Constitucional** (Constituição da República Portuguesa)
  - Contém os princípios gerais nas diversas matérias do nosso ordenamento jurídico, sendo que o seu desenvolvimento cabe às leis ordinárias
- Segundo: Leis Ordinárias (por ordem hierárquica)
  - **Lei**: proveniente da Assembleia da República
  - **Decreto-Lei**: proveniente do Governo
  - **Decreto Regulamentar**: proveniente do Governo, precisa de ser promulgada pelo Presidente da República
  - **Resolução do Conselho de Ministros**: proveniente do Governo, têm de ser assinada por todos os Ministros
  - **Portaria**: proveniente do Governo, apenas tem de ser assinada por um Ministro
  - **Despacho Normativo**: proveniente do Governo e constitui uma ordem dada pelo Ministro para ser aplicada no interior do ministério

Obediência dos diplomas legais

- Relação entre diplomas legais: cada uma das várias modalidades de leis ordinárias deve obediência à constituição e às outras leis ordinárias que lhe são superiores em termos hierárquicos
- Em consequência, existem dois tipos de **vícios**:
  - Vício de **inconstitucionalidade**: violação do disposto na Constituição
    - Inconstitucionalidade material/objetiva: quando tenham sido infringidos os princípios consignados na Constituição (pode ocorrer antes da sua promulgação)
    - Inconstitucionalidade formal: quando se trata quer da competência da autoridade que emitiu a norma jurídica, quer das formalidade preceituadas para a elaboração, votação e promulgação das leis (pode ocorrer antes ou depois da sua promulgação)
  - Vício da **ilegalidade**: deriva da violação de leis ordinárias, hierarquicamente superiores

Tipos de leis

- Civil
  - governa a nação e o estado
  - gere as relações e os conflitos entre as entidades organizacionais e as pessoas
- Criminal
  - lida com as violações que afetam a sociedade
  - assegura a ordem de forma ativa, pelo estado
- Privada
  - regula os relacionamentos entre indivíduos e organizações
- Pública
  - regula a estrutura/administração do governo e administração pública central e local e da relação com os cidadãos, funcionários públicos e outros governos

Luís Borges Gouveia, lmbg@ufp.edu.pt

Legislação nacional

- Principais leis no contexto nacional
  - Constituição (1976)
  - Código civil (1966)
  - Código penal (1982)
- Igualmente relevantes
  - Código comercial (1888)
  - Código de processo civil (1961)
  - Código de processo penal
  - Código do trabalho
  - Código administrativo (1940)

Constituição da República Portuguesa

- Art.º 26ª:
  - A todos são reconhecidos os direitos à identidade pessoal... ao bom nome e reputação, à imagem… à reserva da vida privada e familiar e à protecção legal contra quaisquer formas de discriminação
- Art.º 35º:
  - 1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua rectificação e actualização, e o direito de conhecer a finalidade a que se destinam, nos termos previstos na lei.
  - 2 . A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua protecção, designadamente através de entidade administrativa independente
  - 3. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, féreligiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos.
  - 6. Os dados pessoais constantes em ficheiros manuais gozam de protecção idêntica à prevista nos números anteriores, nos termos da lei
  - Texto integral da Constituição (VII Revisão Constitucional, 2005) *http://www.parlamento.pt/Legislacao/Documents/constpt2005.pdf*

Lei de proteção de dados (LPD)

- A primeira lei de proteção de dados portuguesa foi a lei n.º 10/91, 29 de Abril;
- Revogada pela Lei de Proteção de Dados Pessoais – Lei n.º 67/98, de 26 de Outubro, que transpôs para a ordem jurídica a Directiva 95/46/CE
  - Lei de proteção de dados: *https://www.cnpd.pt/bin/legis/nacional/LPD.pdf*

Lei n.º 103/2015 de 24 de agosto

- Artigo 7.º: Aditamento à Lei n.º 67/98, de 26 de outubro
- É aditado à Lei n.º 67/98, de 26 de outubro, o artigo 45.º A, com a seguinte redação:
- "*Artigo 45.º -A Inserção de dados falsos*
  - *1. Quem inserir ou facilitar a inserção de dados pessoais falsos, com a intenção de obter vantagem indevida para si ou para outrem ou para causar prejuízo, é punido com pena de prisão até 2 anos ou com pena de multa até 240 dias.*
  - *2. A pena é agravada para o dobro se da alteração referida no número anterior resultar efetivo prejuízo para uma pessoa*."

A CNPD (*http://www.cnpd.pt*)

- Entidade administrativa independente, com poderes de autoridade, que funciona junto da Assembleia da República
- Tem como atribuição controlar e fiscalizar o cumprimento das disposições legais em matéria de protecção de dados pessoais, em rigoroso respeito pelos direitos do homem e pelas liberdades e garantias consagradas na Constituição e na lei
- Compete-lhe em especial:
  - Emitir pareceres sobre disposições legais;
  - Autorizar tratamentos de dados pessoais;
  - Autorizar, excepcionalmente, a utilização de dados para finalidades não determinantes da recolha
  - Autorizar interconexões e transferências de dados pessoais para países terceiros;
  - Fixar o tempo de conservação dos dados
- Lei orgânica da Comissão Nacional de Proteção de Dados
  - Lei 43/2004: *https://www.cnpd.pt/bin/cnpd/Lei_43_2004.pdf*

Outra legislação relevante

- Cartão do cidadão: lei 7/2007 *https://www.cnpd.pt/bin/legis/nacional/Lei7-2007-cartao-cidadao.pdf*
- Cibercrime: lei 109/2009 *https://www.cnpd.pt/bin/legis/nacional/LEI109_2009_CIBERCRIME.pdf*
- Saúde: lei 12/2005 *https://www.cnpd.pt/bin/legis/nacional/Lei12-2005.pdf*
- Comunicações eletrónicas:
  - Lei 41/2004 Regula a proteção de dados pessoais, republicada em 2012 https://www.cnpd.pt/bin/legis/nacional/Lei_46_2012.pdf
  - Lei 32/2008 – transpõe a Diretiva da Retenção de Dados, relativa à conservação de dados *https://www.cnpd.pt/bin/legis/nacional/Lei32-2008_retencao_dados.pdf*

CNPD

- Aprecia queixas e reclamações
- Aplica coimas
- As suas decisões tem força obrigatória
- Para cumprir as suas funções pode:
  - Aceder aos sistemas informáticos, ficheiros de dados pessoais e toda a documentação relacionada
- As entidades públicas e privadas tem o dever de colaborar com a CNPD

Autoridade Europeia de Proteção de Dados

- Site da autoridade
  https://secure.edps.europa.eu/EDPSWEB/edps/EDPS?lang=pt
  - Artigos:
    https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Publications/Papers
  - Relatórios anuais:
    https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Publications/AR
  - Brochuras:
    https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/Factsheets

Outros recursos

- Comissão Europeia – unidade de proteção de dados:
  - *http://ec.europa.eu/justice/data-protection/index_en.htm*
- Comissão Europeia – Justiça, proteção de dados:
  - *http://ec.europa.eu/justice/data-protection/*
- Agência Espanhola de Proteção de Dados:
  - *http://www.agpd.es*
- Organização para cooperação e desenvolvimento económico:
  - *http://www.oecd.org/careers/dataprotectionpolicy.htm*
- Departamento de Comércio dos EUA
  - *http://www.export.gov/safeharbor/*
- United Nations Commission for the protection of privacy
  - *https://www.privacycommission.be/en*

Conceito de dados pessoais

- Qualquer informação, de qualquer natureza, independentemente do suporte, incluindo som e imagem, relativa a uma pessoa identificada ou identificável.
- É considerada identificável, a pessoa que direta ou indiretamente se possa identificar, designadamente por referência a um número, ou qualquer elemento específico da sua identidade física, psíquica, fisiológica, económica, cultural ou social

Dados sensíveis

- É proibido o tratamento de dados pessoais referentes a convições filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem racial ou étnica, bem como o tratamento de dados relativos à saúde e à vida sexual, incluindo os dados genéticos

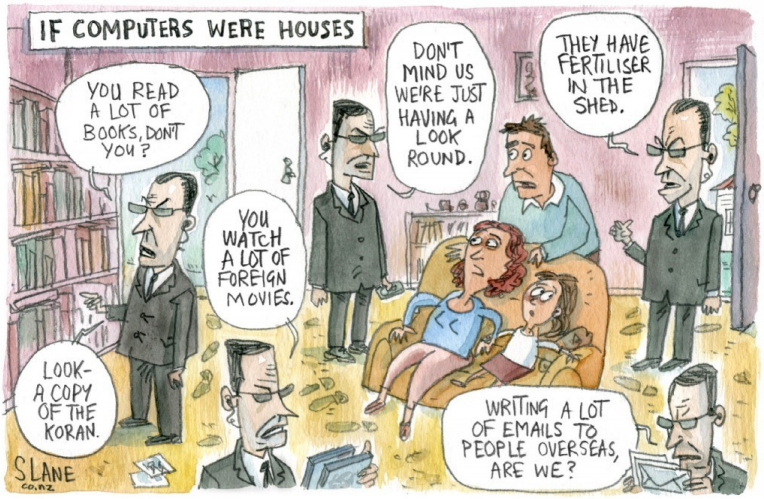
A "elasticidade" da noção de dados sensíveis

- A deliberação n.º 58/2003 da CNDP
  - Dados sobre frequência escolar, incluindo eventuais reprovações
  - Dados sobre medicamentos consumidos
  - Dados sobre sentimentos, sintomas de ansiedade; questões sobre suicídio

Quando se pretende utilizar dados pessoais (sensíveis e não sensíveis)

- Obrigações dos responsáveis:
  - Notificar o tratamento de dados pessoais à CNPD
  - Assegurar os direitos aos titular dos Dados
  - Garantir a segurança da informação
- Direitos dos titulares dos dados:
  - Direito de informação
  - Direito de acesso
  - Direito de correcção
  - Direito de eliminação

O digital e os desafios da proteção de dados (que privacidade é possível com o digital?)



http://www.risk-intelligence.co.uk/the-ethics-of-indiscriminate-surveillance/

(novo) regulamento geral de proteção de dados (rgpd)

- Jornal Oficial da União Europeia (PDF com 88 páginas em…) *https://www.cncs.gov.pt/content/files/regulamento_ue_2016-679_-_protecao_de_dados.pdf*
- REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)
  - publicado a 4 de Maio de 2016
  - entra em vigor a 25 de Maio de 2016
  - Período transitório: 2 anos (a terminar em 25 de Maio de 2018)
  - O regulamento é diretamente aplicável aos 28 Estados Membros, sem necessidade de qualquer transposição para cada jurisdição garantindo a harmonização legislativa ao nível da proteção de dados em todos os países na UE
- Sobre o rgpd e a sua génese (Conselho Europeu): *http://www.consilium.europa.eu/pt/policies/data-protection-reform/data-protection-regulation/*

(novo) regulamento geral de proteção de dados (rgpd)

- introduz alterações significativas às regras actuais de Protecção de Dados impondo às organizações novas obrigações, cujo incumprimento é punido por elevadas coimas que podem ascender a 4% da facturação anual global ou a €20.000.000,00
- Introduz a nível organizacional:
  - os deveres de accountability
  - a realização de Privacy Impact Assessments (PIA)
  - a notificação obrigatória às Autoridades de Proteção de Dados (CNPD) em caso de data breaches
  - a nomeação de Data Protection Officers
  - o reforço da segurança dos dados
- clarifica o conceito de dados pessoais, com novos direitos para os titulares dos dados, como o direito à portabilidade dos dados, o direito ao esquecimento e o direito de oposição a Profiling
- as regras para obtenção do consentimento dos titulares passam a ser muito mais exigentes.
- Introduz os princípios e conceitos que devem nortear os tratamento dos dados como a Privacy by design and by default, ou a pseudonimização dos dados
- O Regulamento abrange além dos Responsáveis pelo Tratamento dos dados (controllers) também os subcontratantes (processors) (alterado da diretiva anterior)
- introduz o conceito de "one stop shop" o que beneficia as organizações que tenham operações em diferentes países da União Europeia
- O Regulamento aplica-se às operações de tratamento que incidam sobre titulares de dados pessoais Europeus, independentemente de o responsável pelo tratamento (ou o subcontratante) se encontrar ou não localizado na UE

Luís Borges Gouveia, lmbg@ufp.edu.pt

10 medidas para aplicação do rgpd (CNPD)

https://www.cnpd.pt/bin/rgpd/10_Medidas_para_preparar_RGPD_CNPD.pdf

1. Informação aos titulares dos dados
2. Exercício dos direitos dos titulares dos dados
3. Consentimento dos titulares dos dados
4. Dados sensíveis
5. Documentação e registo de atividades de tratamento
6. Contratos de subcontratação
7. Encarregado de proteção de dados
8. Medidas técnicas e organizativas e segurança do tratamento
9. Proteção de dados desde a conceção e avaliação do impacto
10. Notificação de violações de segurança

Luís Borges Gouveia, lmbg@ufp.edu.pt

EU Data Protection Regulation

http://www.smartinsights.com/marketplace-analysis/digital-marketing-laws/marketing-implications-of-the-eu-general-data-protection-regulation-gdpr/

Proteger os dados

CRIPTOGRAFIA

Criptografia

- É o esforço de manter privada uma dada informação de modo a que esta seja ilegível para outra outros a quem não seja permitido o acesso (não possibilitado pela falta de uma chave adequada para o efeito)
  - O termo criptografia surgiu da fusão das palavras gregas *kryptós* – oculto e *gráphein* – escrever
  - Conjunto de conceitos e técnicas para codificar uma informação de forma a que somente o emissor e o recetor possam ter acesso a esta, evitando que terceiros (intrusos) a possam interpretar

Origem da criptografia

- Julga-se que Júlio César (imperador Romano) foi o primeiro a utilizar a criptografia como meio de esconder informações secretas
- Chave da correspondência de criptagem, baseada na rotação de 2 letras do abecedário para a esquerda
  - A B C D E F G H I J L M N O P Q R S T U V X Z
  - C D E F G H I J L M N O P Q R S T U V X Z A B
  - Rotação de 2 letras para a esquerda…
- Exemplo
  - Segurança da informação
  - Ugixtcpec fc lphqtocecq

A evolução das comunicações tornou os sistemas manuais (e pouco fiáveis) de criptografia obsoletos

- O uso de comunicações rádio na 1ª Grande Guerra Mundial, tornou evidente a necessidade de novas tecnologias
  - Muitos dos métodos de encriptagem tinham limitações quando um grande número de mensagens eram capturadas com a mesma chave, permitindo a sua descodificação

Roda Vigenère (Guerra Civil)

Roda de cifra M-94, Exército EUA

Enigma: a máquina de criptografia ícone que foi utilizada pela Alemanha durante a WWII

- Inventada por Hengel e Spengler em 1915 (Marinha Holandesa)
  - No entanto, patente Alemã de 1918 por Scherbius que a vende ao Exército (3 rotores) e Marinha (4 rotores)
- Crucial no esforço de guerra e elemento determinante na vitória dos aliados, após decifrar códigos da Enigma
  - Permitia explorar 3.28 X 10^{114} combinações possíveis

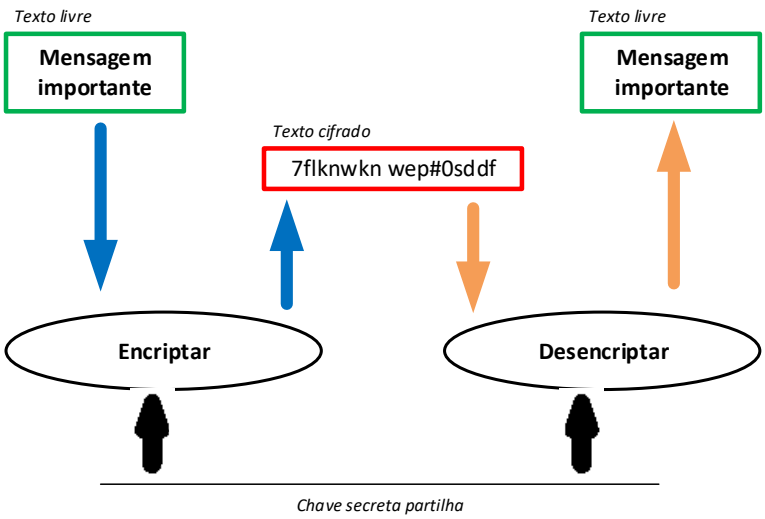
Para saber mais, http://ciphermachines.com/enigma.ppt

Motivos para o recurso à criptografia

- Envio de documentos confidenciais, como contratos ou informação pessoal
- Informação de novos produtos com parceiros
- Comunicação com sua base de fornecedores
- Trocas de informações de natureza financeira
- Troca de e-mails
- A Internet, basicamente, não é uma rede segura
- (home)banking e pagamentos on-line
- Controle de acesso – Canais de TV
- Proteção de dados…

Luís Borges Gouveia, lmbg@ufp.edu.pt

Encriptar e desencriptar



Luís Borges Gouveia, lmbg@ufp.edu.pt

Tipos de criptografia

- Chave secreta
  - Forma tradicional de criptografia – **Simétrica**
  - Chave única para criptografar e decriptografar
  - As duas partes precisam concordar com a chave antes de trocarem informações
  - Usada em ambiente de utilizador único
- Chave pública
  - Forma alternativa de criptografia – **Assimétrica**
  - A chave precisa ser enviada separadamente
  - Sistema permite também separar as funções de codificação da mensagem (criptografar) e de descodificação da informação (decriptografar)

Luís Borges Gouveia, lmbg@ufp.edu.pt

Aplicações de criptografia

- Obrigando (e abrigando) a privacidade
  - Permite ocultar a informação, criptografando as mensagens e tornando estas, ilegíveis a terceiros
  - armazenar o valor codificado das senhas para garantir a sua segurança e assim adicionar mais um nível para a segurança da informação
- Critografar mensagens de correio eletrónico
  - *Pretty Good Privacy* (PGP) e *Secure Multipurpose Internet Mail Extension* (S/MINE)
- Existem diferentes tecnologias de criptografia
  - De maior e menor sofisticação (com usos civis e militares)
  - Implementadas por software em algoritmos, programas e aplicações próprias
  - Implementadas em software por equipamentos dedicados ou como complemento eletrónico de equipamentos existentes
- Assinaturas digitais
  - Permite tornar o documento eletrónico legalmente utilizável, é necessário ter um mecanismo que forneça um meio de autenticar o autor de um documento
  - Necessita de usar chaves públicas
  - Regime jurídico dos documentos eletrónicos e da assinatura: Decreto-Lei nº 88/2009, de 9 de Abril

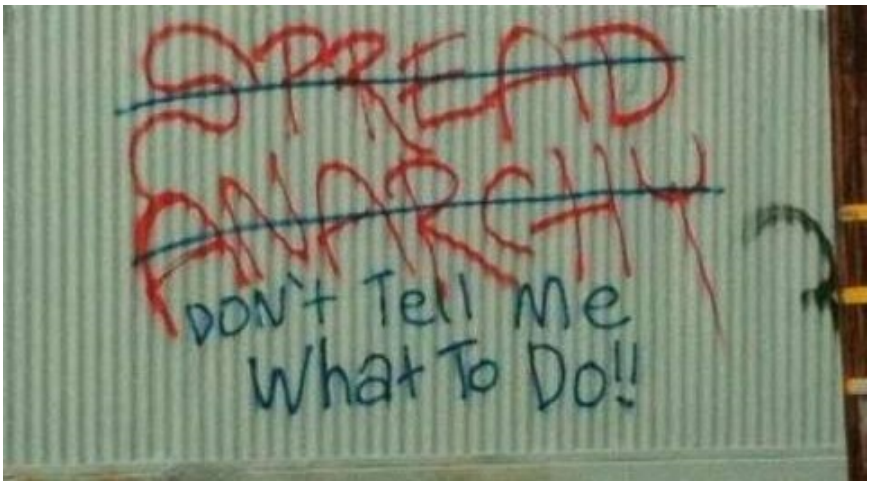
Luís Borges Gouveia, lmbg@ufp.edu.pt

Seguro, mas disponível e funcional

3. **Equilíbrio** entre segurança da informação e proteção de dados individuais
   - 3.1. Proteger dados e informação nas organizações
   - 3.2. Proteger dados e informação de atividade e clientes
   - 3.3. Desafios éticos da proteção de dados
   - 3.4. Enquadramento legal, operações e informações

SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS INDIVIDUAIS

"*A verdadeira liberdade está em fazermos coisas*"
(LMBG 2015)



Luís Borges Gouveia, lmbg@ufp.edu.pt

Princípios de bom senso…

Por maiores que sejam as necessidades de segurança, tem de permitir a atividade corrente de indivíduos e organizações

e

Os custos de segurança tem de ser sempre compatíveis com o retorno potencial de dados e informação protegidos (e claro, compatíveis com o retorno do negócio que suportam e defendem)

Luís Borges Gouveia, lmbg@ufp.edu.pt

A disrupção digital já aconteceu…

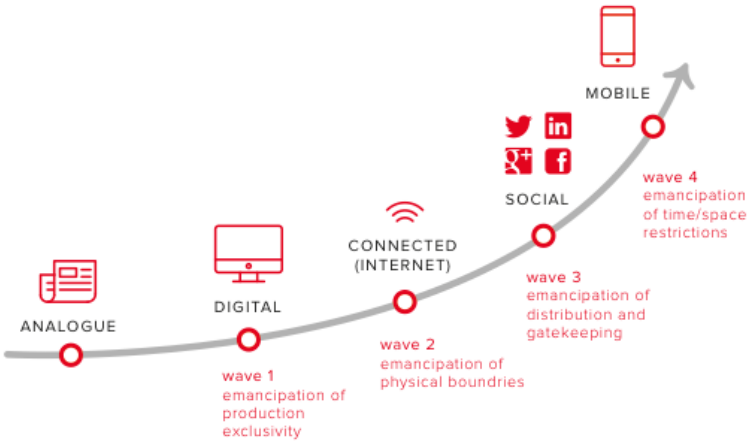
- A maior empresa de táxis do mundo, não tem táxis
  - Uber (http://www.uber.com/)
- O maior fornecedor de camas não possui propriedades
  - Airbnb (https://www.airbnb.com/)
- A maior empresa de telefones do mundo, não possui infraestruturas de telecomunicações
  - Skype (http://www.skype.com/)
- O mais valioso retalhista do mundo não possui inventário
  - Alibaba (http://www.alibaba.com/)
- O mais popular dono de media, não criar conteúdos
  - Facebook (https://www.facebook.com/)
- O banco com maior crescimento não possui dinheiro corrente
  - SocietyOne (https://www.societyone.com.au/)
- A maior cadeia de salas de cinema do mundo, não possui cinemas
  - Netflix (https://www.netflix.com)
- Os maiores vendedores de software não desenvolvem software
  - Apple (http://www.apple.com/) e Google (http://www.Google.com)

Muitos dos desafios, são dilemas

- A transformação digital e a continuidade de negócio
- O jogo da informação para obter conhecimento
- A questão da privacidade versus a segurança
- A necessidade de um plano de segurança
- A importância das pessoas e do conhecimento

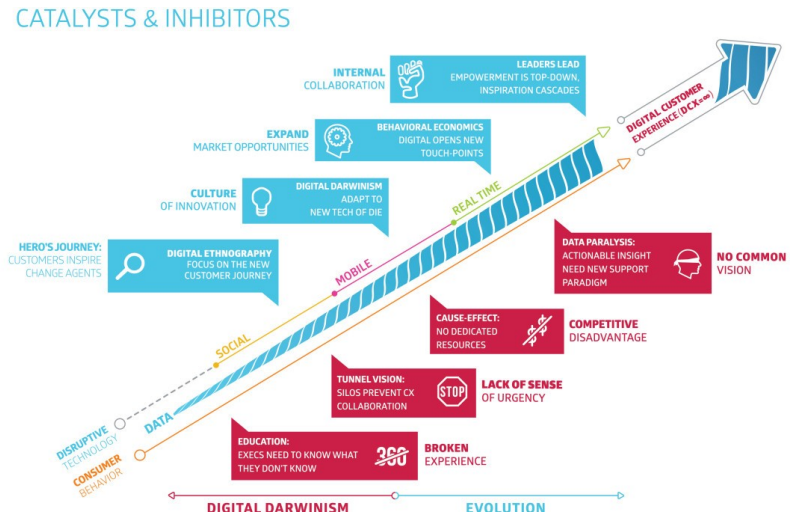
- Resolver situações ou dar resposta a contextos particulares requer por vezes equilíbrios que resultam de muitas das questões serem faces opostas da mesma moeda

Quatro vagas de exploração do digital



http://www.digitaltransformationbook.com/the-speed-of-change-4-waves-of-digital-acceleration/

A transformação digital está a constituir uma prioridade para as organizações



http://www.nearfuture.io/its-about-people-not-technology/

PRIVACIDADE NA INTERNET

Luís Borges Gouveia, lmbg@ufp.edu.pt

Privacidade na Internet

- Pegadas na rede (*digital footprint*)
  - Não existe anonimato na Internet
  - Navegar na Internet revela muito sobre o utilizador (nome do navegador (*browser*), sistema operativo, idioma preferido, website que foi visitado por último, resolução de ecran e número de cores, etc…)
- COOKIES
  - arquivo guardado no computador do utilizador que contém informações específicas do site. Pode conter informações sobre a senha requerida por certo website, um nome de utilizador, um endereço de e-mail ou informações de compra, de perfil e outros elementos de estado
- Os dados de clientes está tornando-se cada vez mais o capital do negócio on-line (os dados como o novo capital)
  - As redes sociais colecionam ao longo do tempo informação complexa sobre individuos e as suas redes de relacioanamento
  - Os grupos de discussão e as redes sociais permitem também criar perfis complexos sobre cada um dos seus utilizadores
- A Internet, por princípio, é um sistema aberto e fornece meios para revelar informação privada, mesmo sem autorização do próprio

Luís Borges Gouveia, lmbg@ufp.edu.pt

Ameaças aos dados

- São vários e de complexidade crescente:
  - Roubo de identidade
  - Captura de dados e informação, não autorizada
  - Acrescento, transformação ou alteração de dados e informação
  - Destruição ou eliminação de dados e informação
  - Deterioração da qualidade de comunicação e de meios de tratamento de dados e informação
  - Bloqueio ou sabotagem de meios e infraestruturas associadas com dados e informação
  - Possibilidade de registo impossível de apagar de informação que pode ser recuperado, sem relacionamento com o texto ou mesmo fora de qualquer contexto

Software malicioso: vírus, *worms* e DoS

- Vírus
  - Pequena peça de software que se anexa a outros programas de forma a ser executado
  - Uma vez executado, espalha-se ao incluir cópias do seu código noutros programas ou documentos
- *Worms*
  - Um programa que se auto replica, semelhante a um vírus de computador
  - Ao contrário de um vírus que se aloja a um executável e se torna parte dele, um *worm* existe por si e não necessita de ser parte de outro programa para se propagar
- Outro tipo de ataque é a negação de serviço
  - DoS, *denial of service* ou DDoS, *distributed denial of service* é um ataque que causa a perda de serviço a utilizadores (normalmente, conetividade de rede e serviços, por via do consumo de largura de banda da vítima ou pela sobrecarga de recursos computacionais do sistema da vítima)
  - Causa perdas por indisponibilidade de serviço ou de informação

Máquinas infetadas

- Os computadores infetados são denominados de *zombies* e constituem um dos meios mais comuns para a distribuição de software malicioso
  - Muito usados para a distribuição de email não desejado, não autorizado ou criminoso (*spam*)
  - Muitos são computadores pessoais, com versões antigas de sistemas operativos (maioritariamente MS Windows), sem anti-vírus ou com estes programas de prevenção, desatualizados
  - Cada vez mais, outro tipo de equipamentos são infetados, como é o caso de dispositivos móveis (em especial, *smartphones*)

Tipos de vírus (de acordo com o método de infeção)

- Vírus de setor de boot
  - Reside no setor de arranque de um sistema de armazenameno de um computador e cada vez que este é inicializado, o vírus é ativado, infetando os ficheiros
- Vírus de execução
  - Trabalham infetando ficheiros executáveis
- Vírus de macros
  - Na maioria dos casos, infetam aplicações mais comuns como os processadores de texto (*MS Word*) e as folhas de cálculo (*MS Excel*)
- Vírus de *script*
  - Baseado no recurso a sequências de instruções usadas como vetores para infeção de equipamentos e programas (recorrem a sistemas de *scripting* como o *MS Visual Basic Scripting Edition* ou o *JavaScript*)

Cavalos de Tróia (*trojan horses*)

- Cavalos de tróia
  - Programa destrutivo que se disfarça de um jogo de computador ou uma qualquer outra aplicação e que, quando executado, afeta e infeta o computador
  - Pode estar associado a um vírus ou a um *worm*
- Especialmente perigosos para a proteção e dados
  - Os cavalos de tróia estão normalmente associados com ferramentas de monitorização de atividade e com sistemas de gravação de ação de teclados (*key loggers*) – úteis para capturar senhas (*passwords*)
  - Podem estar associados a sistemas software, hardware ou mistos

Nível de danos de vírus

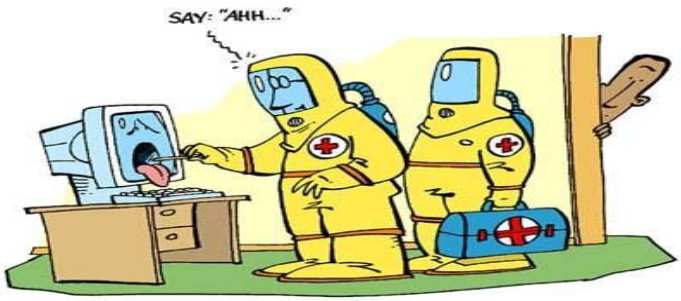
- Nível 1: aborrecedor
  - Exibe mensagens na tela, **sem dano real**
- Nível 2: inocente
  - Exibe mensagens em sua tela e impede a execução de programas, mas **sem dano permanente**
- Nível 3: prejudicial
  - **Destrói os dados do programa infetado**, mas todos os outros dados permanecem intactos
- Nível 4: destrutivo
  - **Destrói todos os dados**, não permite a execução do computador
- Nível 5: raptor
  - **Toma o controlo do computador**. Permite usar o computador como um *zombie* ou como uma brecha (quebra) interna de segurança

Estratégia para combater vírus de computador

- Programas anti-vírus
  - Instalar em cada computador e em cada nível de rede (*firewall*), fornecendo atualizações constantes
- Estratégia de cópias de segurança *(backups)*
  - Manter o hábito de efetuar cópias de segurança regulares. Não deixar de verificar a existência de vírus também nas cópias
- Educação dos utilizadores
  - Organizar cursos introdutórios
  - Manter informação sobre o tema em local útil para facilitar o seu uso, incluindo uma lista de perguntas mais frequentes (FAQ – *frequentely asked questions*)
  - Informar e treinar os utilizadores

Padrões mínimos que deve ter um anti vírus

- *Scanner*: rastreia todos os ficheiros nos discos rígidos locais, disquetes e drives de rede (ou outros meios de armazenamento)
- Proteção: verifica e procura vírus enquanto são carregados ficheiros de dados e programas da Internet, ou é inserido um meio de armazenamento
- Limpador: uma vez que um vírus seja localizado, precisa ser removido, rastreando a base de dados por vacinas ou antidotos



Centro Nacional de Cibersegurança Portugal (http://www.cncs.gov.pt/). Tipos de eventos de segurança

Tipo	Tipo	Tipo
Malware	Botnet drone	Ransomware
Malware configuration	C&C	DDoS
Scanner	Exploit	Brute-force
IDS alert		
Defacement	Compromised	Backdoor
Dropzone		
Phishing	SPAM	
Vulnerability service		
Other		

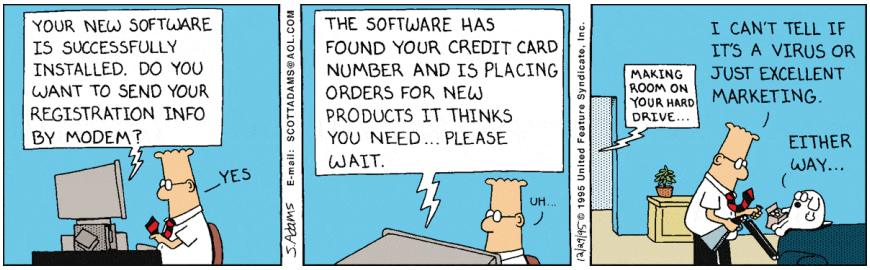
Luís Borges Gouveia, lmbg@ufp.edu.pt

Centro Nacional de Cibersegurança Portugal (http://www.cncs.gov.pt/). Classificação de incidentes

Classe de incidente	Tipo de incidente
Código malicioso	Infeção Distribuição C&C Outro
Disponibilidade	DoS/DDoS Sabotagem
Recolha de informação	Scan Sniffing Phishing
Tentativa de intrusão	Exploração de vulnerabilidade Tentativa de login
Intrusão	Exploração de vulnerabilidade Compromisso de conta
Segurança da informação	Acesso não autorizado Modificação/remoção não autorizada
Fraude	Utilização indevida ou não autorizada de recursos Utilização ilegítima de nome de terceiros
Conteúdo abusivo	SPAM Direitos de autor Pornografia infantil, racismo e apologia da violência
Outro	

Luís Borges Gouveia, lmbg@ufp.edu.pt

Roubo de dados e de identidade tem um enorme impacte económico



GUERRA DA INFORMAÇÃO

Guerra da Informação

- Oficialmente não existe guerra da informação
  - …mas todos os governos desenvolvem mecanismos para proteção em caso de um ataque
- A guerra da informação pode ser conduzida em três níveis diferentes:
  - Pessoal (indivíduo)
  - Corporativo (grupos ou comunidades)
  - Global (sociedade)
- Métodos semelhantes: ataque à privacidade de pessoas, empresas ou países
  - Quem ataca tenta descobrir informação dos outros
  - A diferença está essencialmente na dimensão do dano
- Os alvos tecnologicamente mais avançados são as mais vulneráveis
  - Por exemplo: atacar um *backbone* (ligação principal da Internet) pode criar muito mais dano do que uma bomba

Armas da Guerra da Informação

- Existe uma multiplicidade de vetores de ataque:
  - *Chipping:* substituir processadores por cavalos de Tróia
  - Bombas EMP (*eletronic magmetic pulse*): destrói os componentes electrónicos
  - Engenharia humana: fingir ser outra pessoa ou tirar vantagem da natureza humana
  - Engarrafamente (negação de serviço): usado para bloquear a comunicação
  - Bombas lógicas: recurso a Cavalos de Tróia para libertar um vírus ou um *worm*
  - Nano máquinas: pequenos robos autónomos que atacam o hardware
  - *Spoofing*: pacotes de e-mails e TCP/IP falsificados que ultrapassam os *firewalls* e outras medidas de segurança
  - Alçapões: mecanismos que permitem a entrada num sistema sem ser notada pelas instalações de segurança
  - Cavalos de Tróia: fragmentos de código que se escondem dentro de programas e executam funções não desejadas
  - Vírus: fragmentos de código que se copiam em um programa ou o modificam
  - *Worms*: programa independente que se copia de um computador para outro
- E essencialmente pessoas com competências e conhecimento para poder desenvolver mecanismos sofisticados

Ciberterrorismo

- O terrorismo é uma ameaça no mundo real e também no ciberespaço
- Não existe nenhuma diferença em motivação entre terroristas e os terroristas cibernéticos
  - ambos têm por objetivo intimidar os outros
- A Internet oferece ao terrorista muitas possibilidades de prejudicar uma instituição e causar alarme social
  - Desligar uma central elétrica, via computador
  - Implicar com sistemas de controlo de segurança e proteção civil
  - Afetar serviços ou modificar páginas Web sobre informação pública
  - Existem muitos exemplos de acontecimentos que mostram não ser apenas algo potencial, mas que acontece

Proteção contra o ciberterrorismo

- Senhas (*passwords*)
  - As senhas não podem (devem…) ser poder ser deduzidas, adivinhadas ou encontradas num dicionário ou em referência direta a contextos
  - São necessárias auditorias para verificar a qualidade de senhas e a sua mudança periódica
- Rede
  - Mudar as configurações de rede assim que as vulnerabilidades se tornem aparentes
  - São necessárias auditorias regulares de rede
- Correções
  - Designar um oficial (responsável) de segurança para a tarefa de subscrição de importantes listas de distribuição, informando todos sobre novas quebras de segurança
  - Participar em grupos de discussão, reportando e discutindo incidentes próprios e alheios
- Auditorias
  - Todo o sistema precisa ser verificado em intervalos regulares

Algumas estratégias de ciberterrorismo

- Ataque de vírus
- Alteração de informação
- Corte de comunicação
- Morte à distância
- Disseminação de informações erradas
- Substituição de identidade e de informação
- Destruição de informação e documentos
- Outros, ainda por descobrir… (a imaginação é o limite)

Luís Borges Gouveia, lmbg@ufp.edu.pt

Alguns dos potenciais alvos

- Aviões comerciais
- Equipamento médico e de suporte à vida
- Centrais de energia e centrais atómicas
- Monitores de presença e vigilância de bebés
- Drones (aviões não tripulados)
- Mecanismos automáticos de proteção (portas de prisão)
- Máquinas ATM (*automatic teller machines*)
- Satélites e serviços de satélite (como o gps)
- Fotografias (roubo, alteração ou divulgação)
- Atendedores de chamadas
- Brinquedos de crianças
- Veículos automóveis
- Dispositivos diversos como eletrodomésticos
- Hotéis e instalações com elevado grau de automatismo
- Televisões inteligentes com câmeras e outros sensores

Luís Borges Gouveia, lmbg@ufp.edu.pt

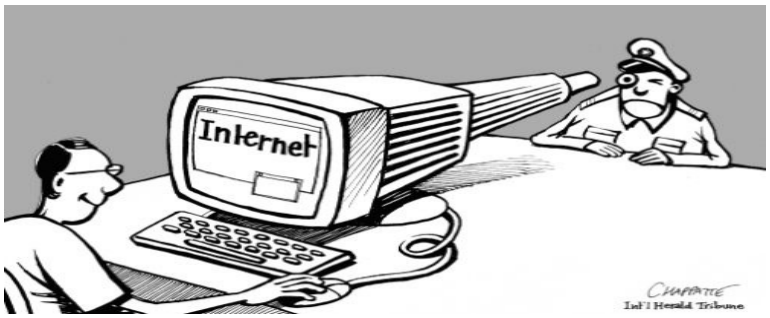
Segurança baseada no lado cliente

- Certificados digitais
  - Ficheiro criptografado e protegido por senha, que inclui informação pessoal sobre o proprietário do certificado
- Cartões inteligentes
  - Têm *microship* embutido em vez de faixa magnética
  - Podem ser de contato, sem contato ou combinados
  - Acesso de informação: leitura, inclusão, modificar ou apagar e execução
  - São utilizados: saúde, finanças, comunicação móvel, telecomunicações e transporte e para identificação de cidadão
- Identificação biométrica
  - Meio de identificar automaticamente as pessoas com base em caraterísticas físicas ou comportamentais
  - Incluem impressão digital, verificação de íris e retina, letra manuscrita, reconhecimento de voz e mão

Segurança baseada no lado servidor

- Necessidade de um *firewall*
  - Sistemas que protegem redes confiáveis de redes não-confiáveis
- Proteção de servidor
  - O sistema de alarme deve ser flexível e permitir ações automatizadas ou interação manual do administrador. O alarme deve ser capaz de enviar *emails*, disparar telefones móveis ou aplicações de alerta
- Ataques internos
  - 80% de todas as quebras são feitas de dentro da empresa, por utilizadores confiáveis
- Protegendo negócios digitais
  - Desconfiar de todas as redes às quais ele está conectado, envolvendo as redes internas, Extranets e a Internet
  - Não faz sentido instalar um *firewall*, se não existe nenhuma política de segurança para disquetes, uso de usb, máquinas de faxe ou telefone
- Sistemas operacionais confiáveis
- Soluções confiáveis

A segurança começa nas pessoas (cultura de segurança)



Luís Borges Gouveia, lmbg@ufp.edu.pt

Materiais complementares para aprofundar os temas em estudo

REFERÊNCIAS

Luís Borges Gouveia, lmbg@ufp.edu.pt

Nuvem de palavras (*www.wordle.net*): exemplo com base num subconjunto das apresentações sobre segurança da informação

Algumas referencias na Web (a adicionar às realizadas ao longo dos slides)

- Centro nacional de cibersegurança: *http://www.cncs.gov.pt/*
- Gabinete Nacional de Segurança: *http://www.gns.gov.pt/*
- Autoridade Nacional de Comunicações: *http://www.anacom.pt/*
- Serviço nacional de informações: *http://www.sis.pt/*
- Comunidade Portuguesa de Segurança da Informação *http://ismspt.blogspot.com/*
- *European Union Agency for Network and Information Security*: *https://www.enisa.europa.eu/*
- *EUA, National White Collar Crime Center*: *http://www.nw3c.org/*
- SDLC, *Security Considerations in the System Development Life Cycle NIST* – USA: *http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf*
- CBK – *Common body of knowledge*, *http://www.isc2.org*
- *OpenLearn: an introduction to information security*: *http://www.open.edu/openlearn/science-maths-technology/computing-and-ict/introduction-information-security/content-section-2.1*

Apresentações do autor, disponíveis na *World Wide Web* (*slideshare*)

- Informação digital e segurança. Ciclo de Conferências sobre Segurança e Cidadania – GNR. Lisboa. 11 de Março de 2015 *http://pt.slideshare.net/lmbg/11mar-gnrlx2015*
- O digital, a mobilidade e a economia da privacidade. Conferência Privacidade, Inovação e Internet. APDSI. Cultugest. Lisboa. 30 de Janeiro de 2015 *http://pt.slideshare.net/lmbg/o-digital-a-mobilidade-e-a-economia-da-privacidade*
- Segurança Informática. Contexto, conceitos e desafios. Rotary Club Vizela. 18 de Junho de 2014 *http://pt.slideshare.net/lmbg/segurana-informtica*
- The Information Warfare – how it can affect us. Rethinking Warfare Conference. UFP, Porto. 10th November 2014 *http://pt.slideshare.net/lmbg/the-information-warfare-how-it-can-affect-us*
- Gestão das organizações, natureza, âmbito e complexidade. INA, Porto. Abril de 2011 *http://pt.slideshare.net/lmbg/gestodas-organizaes-natureza-mbitoe-complexidade*

Luís Borges Gouveia, lmbg@ufp.edu.pt

Termos explicados associados com a segurança da informação e proteção de dados

GLOSSÁRIO

Luís Borges Gouveia, lmbg@ufp.edu.pt

Glossário de termos

- ***Big data***: quantidades massivas de dados recolhidas ao longo do tempo e que se podem analizar com ferramentas de bases de dados tradicionais. Para o seu tratamento, recorre-se a equipamentos de grande poder de processamento e a técnicas de inteligência artificial. Estes dados incluem transações comerciais, textos não estruturados, documentos da Web (blogues e de redes sociais), mensagens de correio eletrónico, fotografias, vídeos, dados de múltiplos sensores e logs de atividade. O objetivo é analizar os dados de forma a estabelecer correlações entre estes, de modo a servir as mais diversas finalidades: segmentação de mercados, construção de perfis de consumidores, análise de risco, luta contra a fraude, análise de mercados financeiros

Glossário de termos

- **Cidades Inteligentes** (smart cities): uma cidade que utiliza e explora as tecnologias de informação e comunicação para conseguir um crescimento económico sustentável, um uso adequado dos recursos naturais e uma maior qualidade de vida para os seus cidadãos, bem como fomentar a participação dos mesmos no governo da cidade
- ***Cloud computing*** (computação em nuvem): conjunto de serviços baseados na *World Wide Web*, em que os utilizadores dispõem de uma grande variedade de capacidades funcionais que pagam apenas na medida em que as usam. Trata-se de um modelo de computação que se baseia na partilha de recursos em rede, em alternativa à utilização de servidores locais e próprios de cada organização

Glossário de termos

- ***Data loss prevention*** (prevenção de perda de dados): produto concebido para detetar potenciais filtros ou acessos não autorizados aos dados de um sistema de infromação. Baseia-se na monitorização, deteção e bloqueio da utilização dos dados, antes de uma atividade suspeita (quer em repouso, quer em utilização ou transmissão).
- **Drones**: veículos aérios não tripulados, guiados por controle remoto
- ***Intrusion Detection System*** (IDS, sistemas de deteção de intrusão): sistema concebido para monitorizar o tráfego de entrada e de saída de um sistema informático, para identificar padrões suspeitos de atividade que possam indicar a possibilidade de um ataque malicioso

Luís Borges Gouveia, lmbg@ufp.edu.pt

Glossário de termos

- **Inteligência Artificial**: ciência que trata da reprodução das caraterísticas da inteligência humana, para os computadores. Também se pode definir como o estudo e conceção de agentes inteligentes (sistemas que percebem o contexto e tomam decisões que maximizam as probabilidades de êxito)
- **Internet das coisas** (IOT, Internet of things): rede de dispositivos interligados através da Internet que se comunicam entre eles
- **Metadatos**: significa literalmente, dados sobre os dados. São dados que descrevem outros dados e que permitem que os mesmos sejam localizados e processados mais facilmente. Por exemplo, quando é realizada uma chamada telefónica, a hora, o número de origem, o número de destino e a duração da ligação são metadados relativos à chamada telefónica e podem ajudar à sua localização e seleção

Luís Borges Gouveia, lmbg@ufp.edu.pt

Glossário de termos

- **Mineração de datos** (Data Mining ou análise de dados): é um processo computacional para a descoberta de padrões comuns e para a extração de informação e conhecimento, analizando grandes volumes de dados com técnicas de inteligência artificial
- **Necessidade de conhecer** (need to know): refere a técnica de controlo de acesso à informação que garante que uma pessoa ou recurso, apenas acede aos dados que sejam estritamente necessários para realizar as suas funções. O obetivo é dificultar o acesso não autorizado à informação , limitando ao mínimo imprescindível as pessoas que tem acesso à informação

Glossário de termos

- ***Privacy by Design*** (privacidade à medida): abordagem à conceção de sistemas de informação que tem em consideração os requisitos de privacidade desde as etapas iniciais até ao uso e exploração dos dados
- ***Privacy Impact Assessment*** (PIA, avaliação de impacte de privacidade): revisão sistemática de um produto, serviço ou sistema de informação para identificar os riscos que podem ocorrer para a privacidade e implementar as medidas necessárias para os mitigar até níveis aceitáveis
- **RFID** (Radio-frequency Identification): recurso a frequências eletromagnéticas para transmitir dados sem fios, entre etiquetas emissoras RFID e leitores eletromagnéticosque os transferem para um computadorpara a identificação e seguimento dos objetos representados pelas etiquetas. Ao contrário dos códigos de barras, esta tecnologia permite ler uma etiqueta que não está no campo de visão do leitor