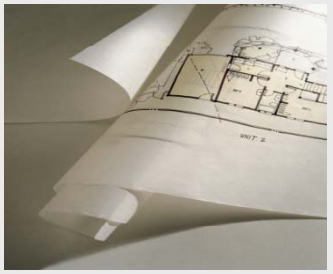






Segurança dos Sistemas de Informação

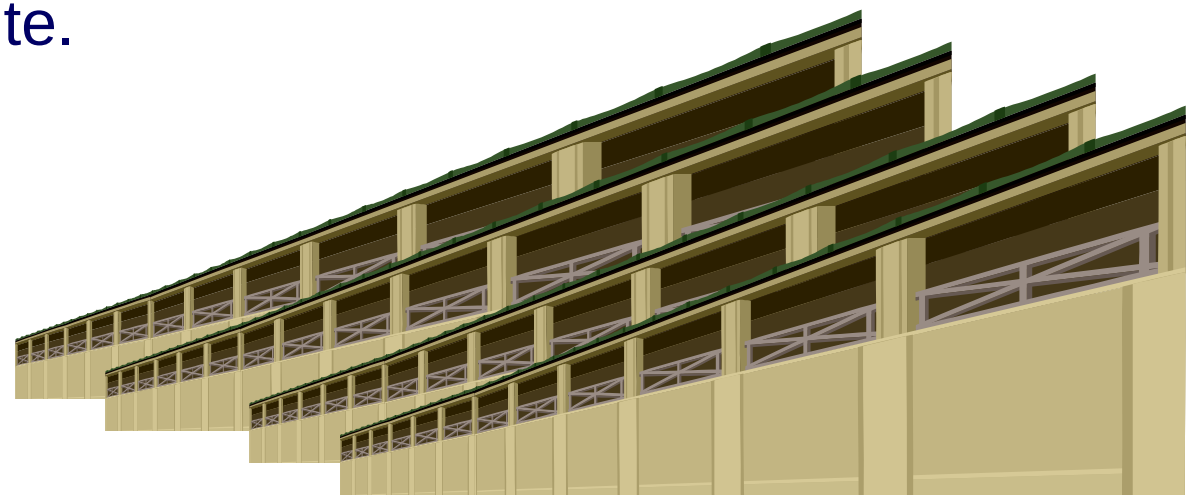
Agenda

- **Introdução**
- **Conceitos**
- **Casos recentes**
- **ISO 27001**
- **O perfil de um CISO**

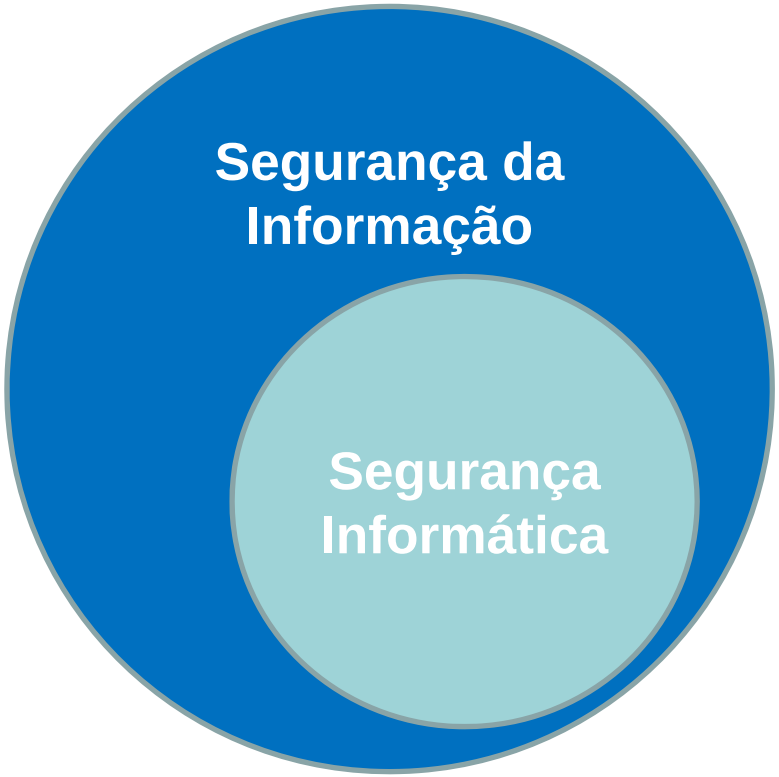
- A Segurança é tão forte como a robustez do elo mais fraco

Defesa em camadas

***Layering**, também conhecido como defesa em profundidade ou em camadas*, baseia-se no conceito de utilização de vários controlos de forma encadeada. Apenas um controlo não garante de forma eficaz a protecção para todas as ameaças. A utilização de uma combinação de controlos permite assim disponibilizar uma solução mais resiliente.



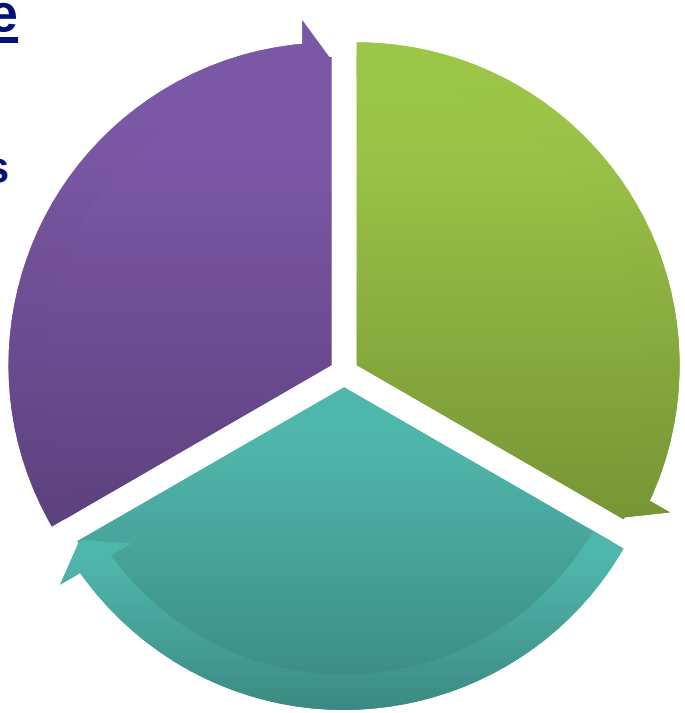
- Segurança da Informação vs Segurança Informática



Os 3 Pilares da Segurança

Confidencialidade

Assegurar que a informação é acedida apenas pelas pessoas autorizadas.



Disponibilidade

Assegurar que os utilizadores autorizados têm acesso à informação sempre que dela necessitarem.

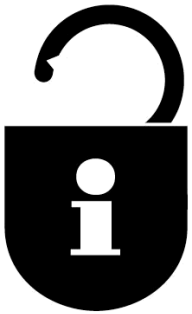
Integridade

Salvaguardar a fiabilidade e a totalidade da informação.

Protecção da Informação

É necessária ao funcionamento do negócio

É factor de distinção (vantagem competitiva)



Requisitos legais

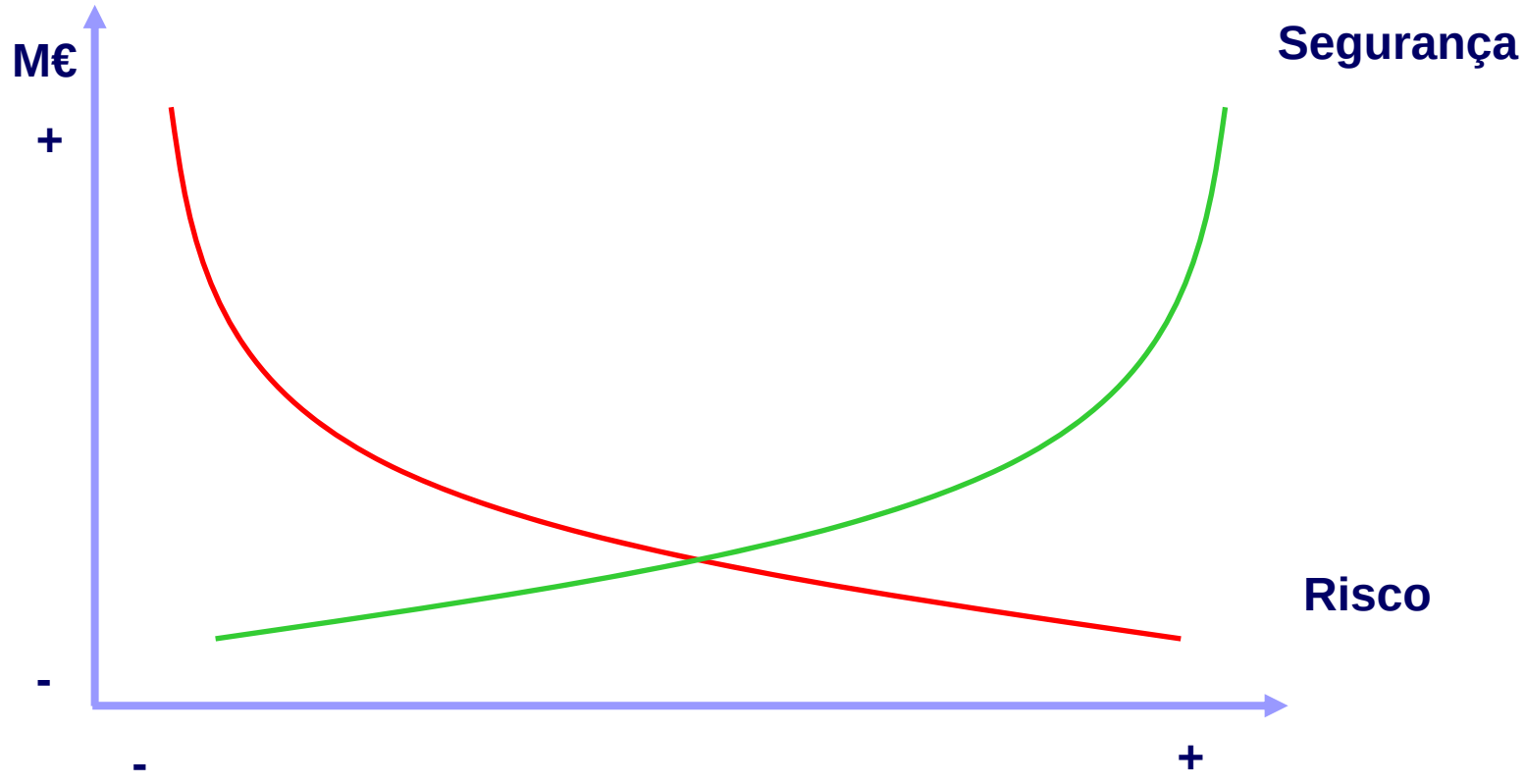
Garante a responsabilização dos colaboradores

Representa o conhecimento da empresa

Serve de suporte à tomada de decisões

Imagem da empresa

A Segurança versus o Risco



Os 10 erros mais comuns dos utilizadores

#1 – Escolher passwords triviais

#2 – Partilhar passwords com outros utilizadores

#3 – Afixar passwords escritas em post-its nos computadores

#4 – Deixar documentos confidenciais nas impressoras

#5 – Deixar documentos confidenciais em cima das secretárias

#6 – Deixar desprotegidos os computadores pessoais sem cadeados

#7 – Não fazer periodicamente backups dos dados

#8 – Executar programas de fontes desconhecidas

#9 – Não utilizar antivírus

#10 – Não utilizar firewall quando se acede à Internet

Perfil do atacante

Caso FreePort

SOL 3a-feira, 3 Março 2009 16º C Máx Lisboa

1º Caderno | Confidencial | Tabu | Essencial | Imobiliário | Edição em pa

macromedia FLASHPAPER 106%

Director
José António Saraiva
Director Adjunto
José António Lima
Subdirectores
Mário Ramires e Vítor Rainho
Edição n.º 129
28 Fevereiro 2009

SOL
TODOS OS SÁBADOS

UM JORNAL QUE VALE POR SI
Preço 2,5 euros IVA incluído
Código de barras no canto inferior direito
www.sol.pt

Pirata atacou ficheiros da Procuradoria

▶ **O ataque foi detectado em computador de um magistrado que investiga o caso Freeport**

UM vírus foi descoberto no computador de um dos magistrados ligados ao Freeport, temendo-se que por esse meio tenham sido subtraídos documentos em segredo de Justiça. Ter-se-á encontrado um novo meio de violar a lei? » Pág. 15

Caso da Heartland

Home » CBS News Investigates

Major Data Breach Puts Millions At Risk

CBS Evening News: Major Credit Card Processor Is Slow To Respond, Hides News From Consumers

Jan. 23, 2009 | by Armen Keteyian

Comments 63

E-MAIL STORY | PRINT STORY | SPHERE | SHARE | TEXT SIZE: A A A

VIDEOS | PHOTOS

(CBS)

RELATED

INTERACTIVE

ID Theft

See how you may be vulnerable, learn about new scams and get tips to protect your good name.

STORIES

AnswerTips™ enabled (What's this?)

(CBS) *If the market meltdown, housing and bank crises weren't enough, U.S. consumers can now add the potential of massive credit and debit card fraud to the list financial concerns. A major processor of credit card transactions just disclosed its system had been hacked, putting millions of consumers at risk, reports* ***CBS News chief investigative correspondent Armen Keteyian*** *reports.*

The cyber-thieves went straight to the heart of one of the biggest and most respected credit and debit card processing companies in the country, Heartland Payment Systems of Princeton, N.J.

"It could be the largest breach ever," said cyber law attorney Andrew DeVore. "It would dwarf the largest prior breach."

Sources tell **CBS News** that hackers cracked Heartland's computers as far back as May of last year. But it wasn't until last week, after being alerted to suspicious activity by Visa and MasterCard, that the company uncovered malicious software in its system.

Caso Société Générale


Diário de Notícias

Edições Anteric

Quinta, 7 de Feverei

Edição Papel

Lisboa 01.02.08

dn.homepage » dn.dnbolsa

DN TEMA
NACIONAL
EDITORIAL
ECONOMIA
OPINIÃO
INTERNACIONAL
SOCIEDADE
DESPORTO
CIDADES
ARTES
MEDIA
DN GENTE
BOLSA
SPORT

Jogo de alto risco na Bolsa derruba Société Générale

ANTÓNIO OLIVEIRA E SILVA, Paris

Controlos do Société Générale antes da fraude falharam, diz ministra

A ministra de Economia e Finanças da França, Christine Lagarde, disse nesta segunda-feira que alguns dos controles internos do banco Société Générale --que sofreu no mês passado uma perda de cerca de **4,9 mil milhões de euros** com um esquema de fraude sobre as operações realizadas pelo operador Jérôme Kerviel falharam ou não foram levados em consideração antes do golpe.

O método utilizado pelo senhor Jérôme Kerviel consistiu na realização de transacções não autorizadas, as quais conseguiu camuflar, alegadamente pela intrusão nos computadores do banco, para a criação de transacções fictícias que compensassem as suas perdas, tendo as suas operações totalizado aproximadamente 50 mil milhões de euros.

Caso da AMD

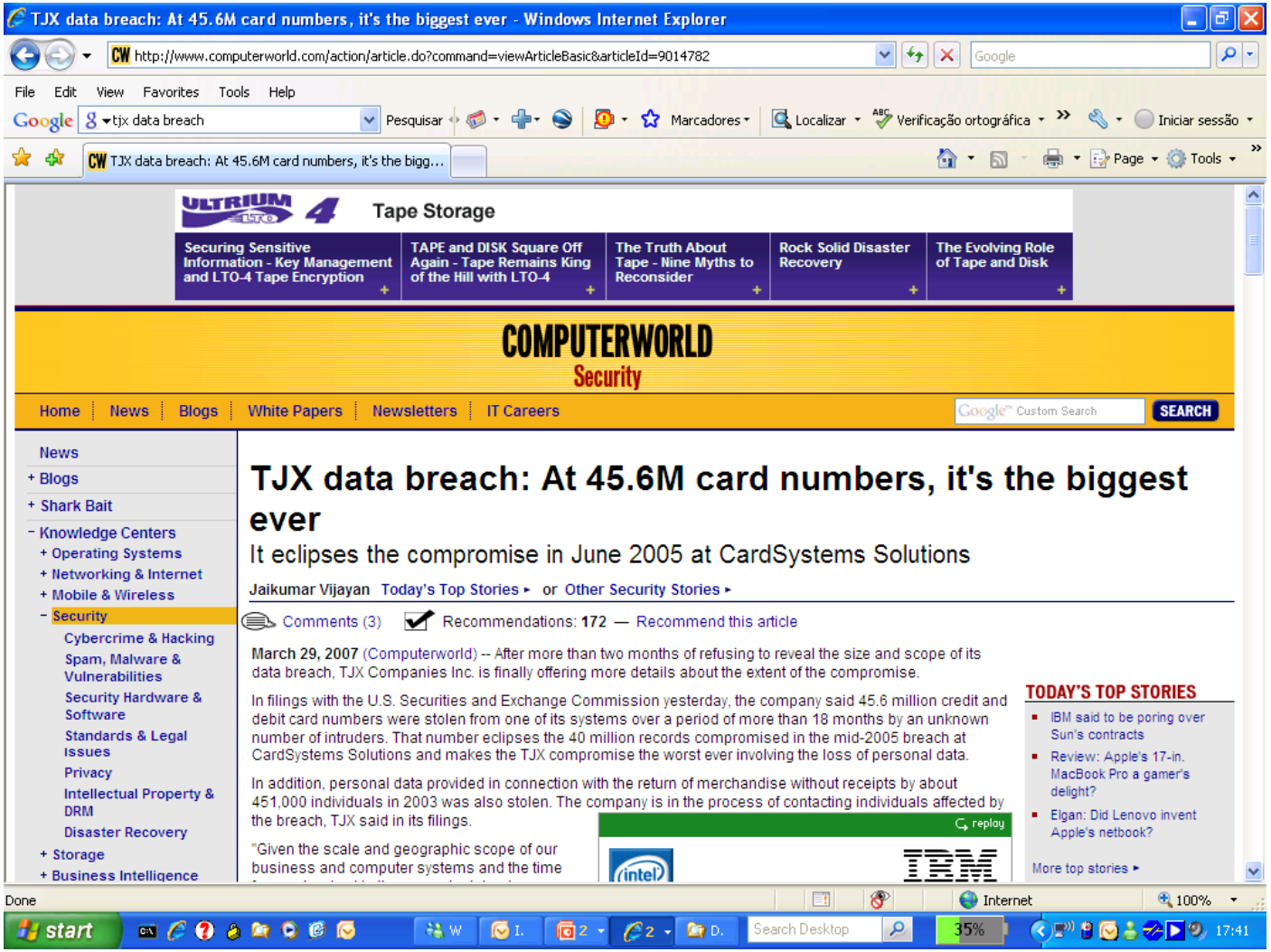
Funcionário da AMD rouba segredos da Intel

Um funcionário da AMD que saiu da Intel é acusado de ter roubado informação sensível aos ex-patrões.

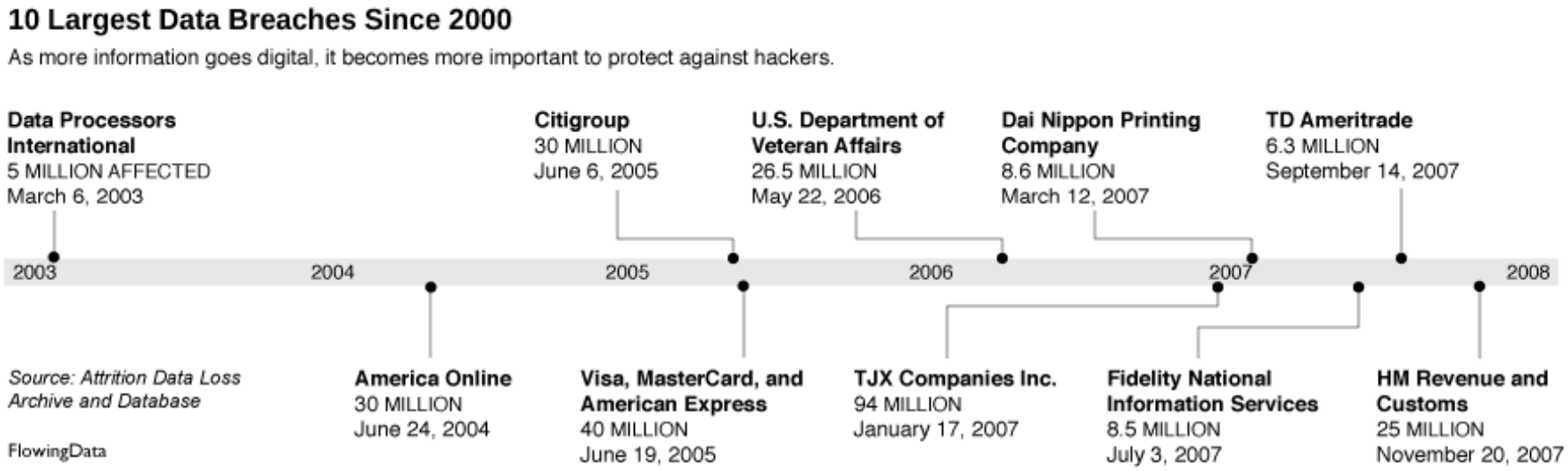
Biswahoman Pani até começou a trabalhar na AMD no dia 2 de Junho, quando o contrato com a Intel só expirava a 10 de Junho, de acordo com a *PC Pro*. Este funcionário disse à Intel que ia sair para entrar numa empresa da área financeira, mas uma vistoria nos sistemas internos mostram que terá descarregado 100 páginas de informação sensível.
A justificação de Pani é que esses documentos seriam para a esposa que se vai candidatar a um trabalho na Intel.

O FBI está a investigar a situação, em conjunto com os dois gigantes dos *chips*.

O caso do retalhista TJX

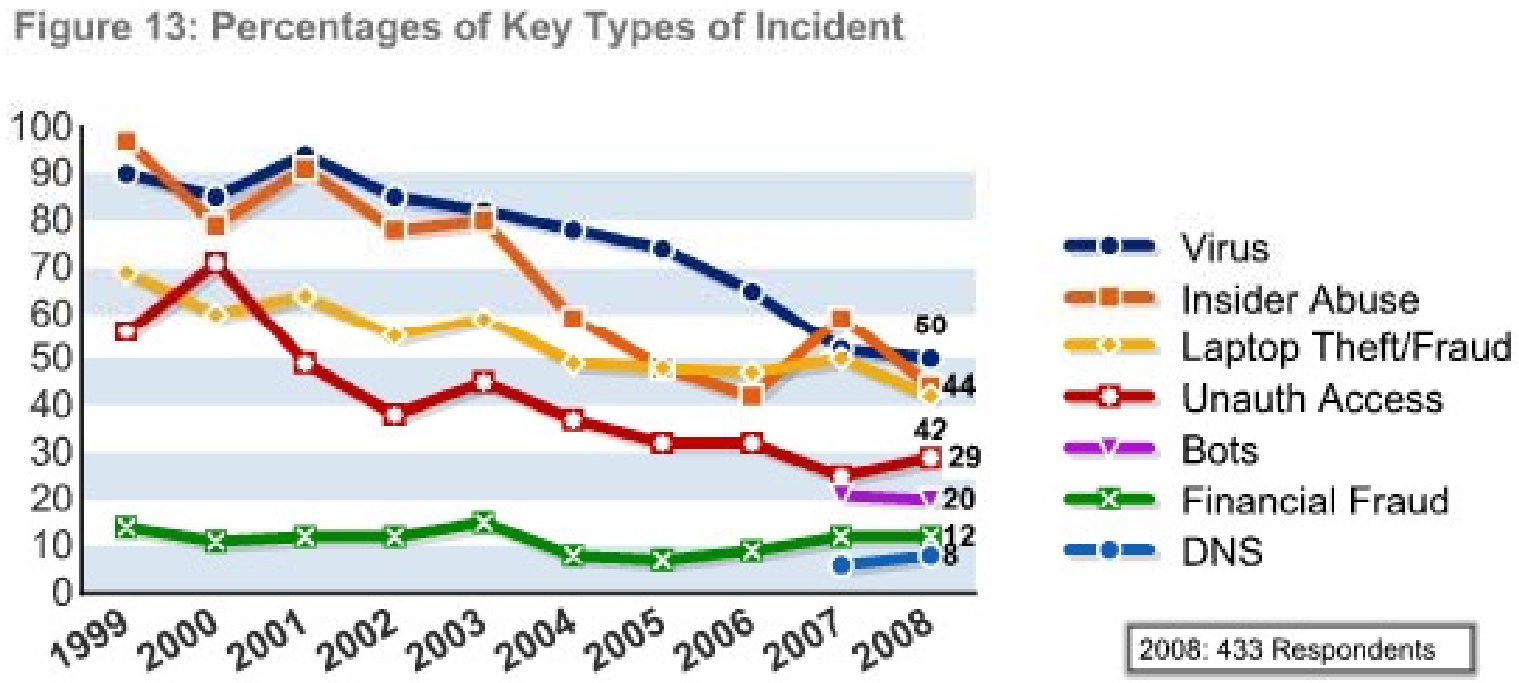


Casos de Fuga de Informação



Fonte: Attrition.org

Principais Riscos Informáticos



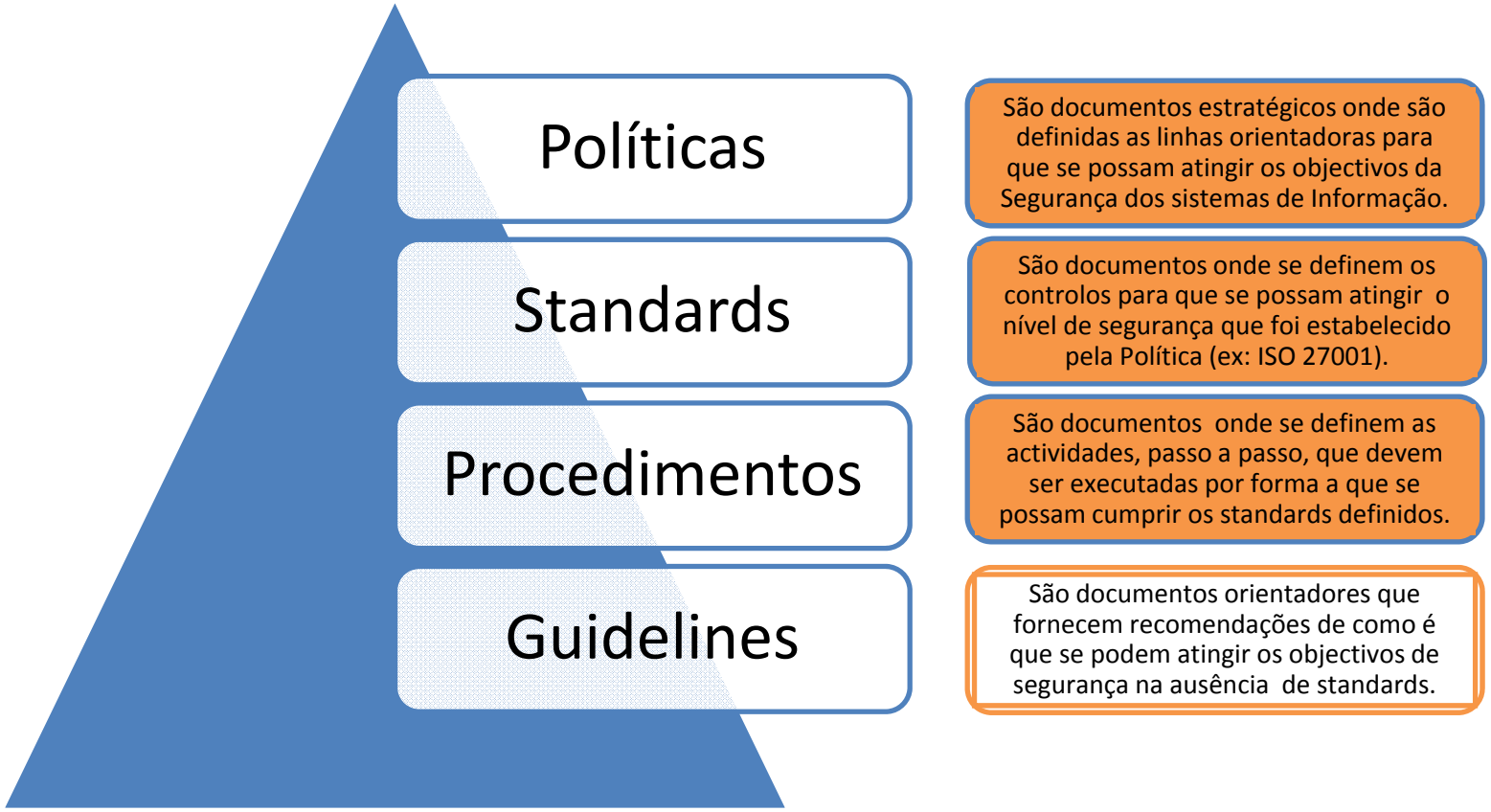
Fonte: 2008 CSI/FBI Computer Crime and Security Survey

Principais Riscos Informáticos

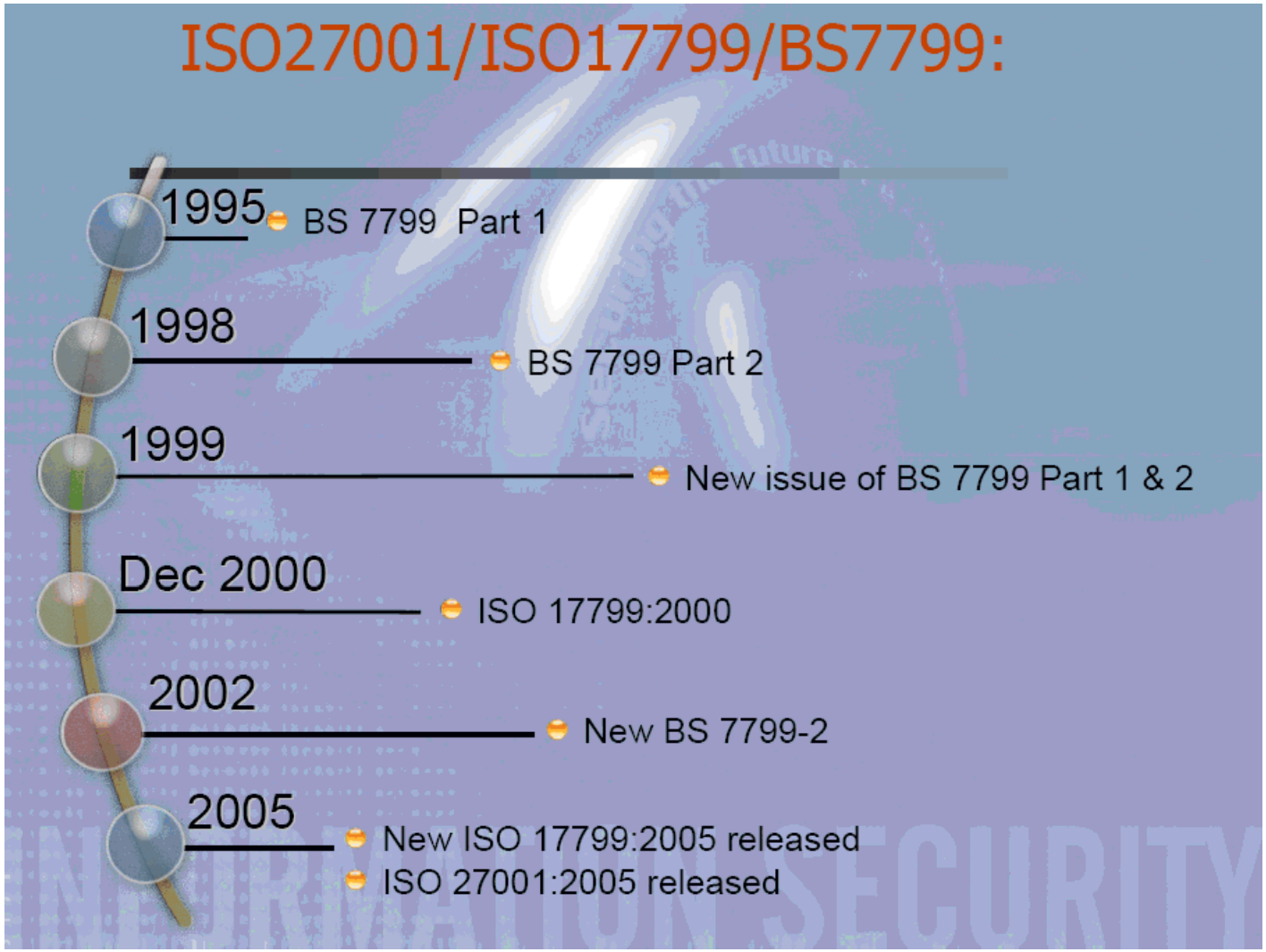
Tabela	2004	2005	2006	2007	2008	Variação
Negação de Serviço	39%	32%	25%	25%	21%	↓
Roubo de Portáteis	49%	48%	47%	50%	42%	↓
Fraude Telecomunicações	10%	10%	8%	5%	5%	
Acesso não Autorizado	37%	32%	32%	25%	29%	↑
Virus	78%	74%	65%	52%	50%	↓
Fraude Financeira	8%	7%	9%	12%	12%	
Abuso Interno	59%	48%	42%	59%	44%	↓
Intrusão de Sistemas	17%	14%	15%	13%	13%	
Sabotagem	5%	2%	3%	4%	2%	↓
Roubo/Perda de Informação Pessoal	10%	9%	9%	8%	9%	↑
- Dispositivos Móveis					4%	
- Outros Dispositivos					5%	
Acesso não Autorizado a Redes Wireless	15%	16%	14%	17%	14%	↓
Alteração das Páginas (Defacement)	7%	5%	6%	10%	6%	↓
Utilização Inadequada de Aplicações WEB	10%	5%	6%	9%	11%	↑
Bots				21%	20%	↓
Ataques ao Domain Name Server				6%	8%	↑
Abuso Messenger				25%	21%	↓
Escuta de Passwords				10%	9%	↓
Roubo/Perda de Dados de Clientes				17%	17%	
- Dispositivos Móveis					8%	
- Outros Dispositivos					8%	

Fonte: 2008 CSI/FBI Computer Crime and Security Survey

Política, Standard, Procedimentos e Guidelines



História dos ISOs 27001/2



ISO/IEC 27000

- As normas ISO 27000 (também conhecidas por 'ISMS Family of Standards‘, englobam os standards de segurança da informação que foram públicados pelo International Organisation for Standardization (ISO)

- Estes documentos oferecem recomendações de melhores práticas na área da gestão da segurança da informação, riscos e controlos dentro do contexto de um Sistema Integrado de Gestão de Segurança ou Information Security Management System (ISMS)

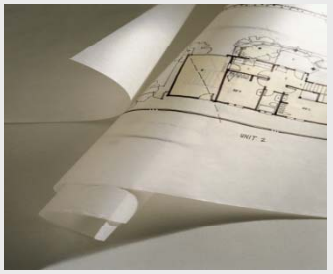
ISO/IEC 27001 vs 27002

ISO 27001	ISO 27002
• Define especificações para estabelecer, implementar, operar, monitorar, auditar, manter e melhorar o Information Security Management System (Baseado no British Standard BS 7799 Part 2, públicado pelo ISO/IEC em 2005)	• Define código de prática, onde se definem orientações para implementar um Information Security Management System (anteriormente conhecido por ISO 17799)
• Pode ser utilizado no processo de avaliação e certificação	• Não pode ser utilizado no processo de avaliação e certificação

ISO/IEC 27001

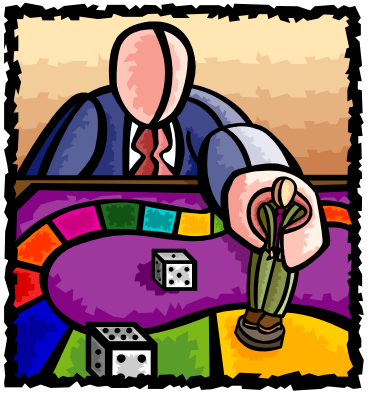






Segurança dos Sistemas de Informação

O perfil de um CISO
(Chief Information Security Officer)



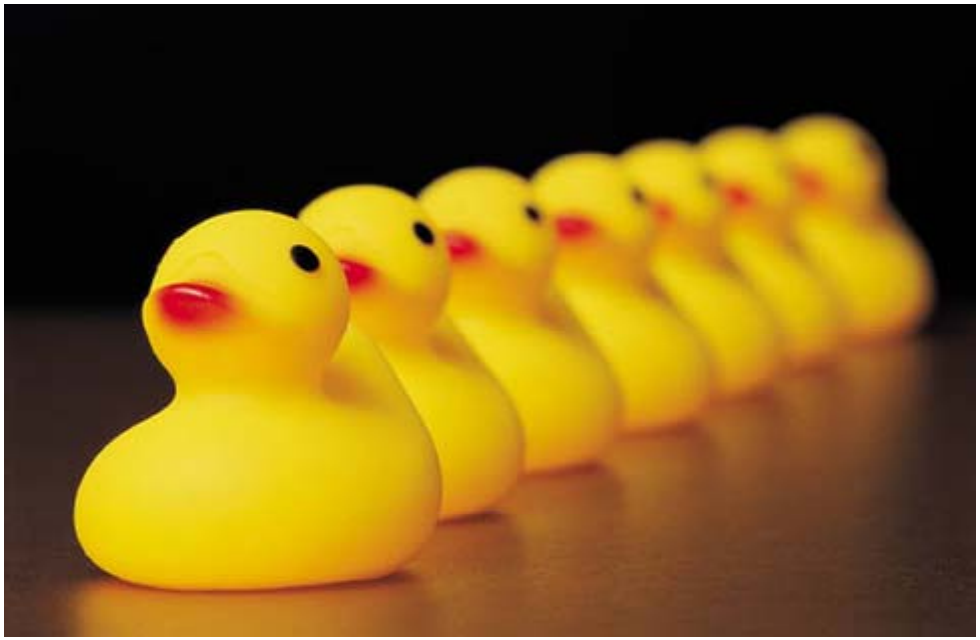
10 características de um CISO

#1 - ASSEGURAR O ENVOLVIMENTO DA GESTÃO

"I know a lot of highly-confidential company secrets, so my boss made me get a firewall installed."

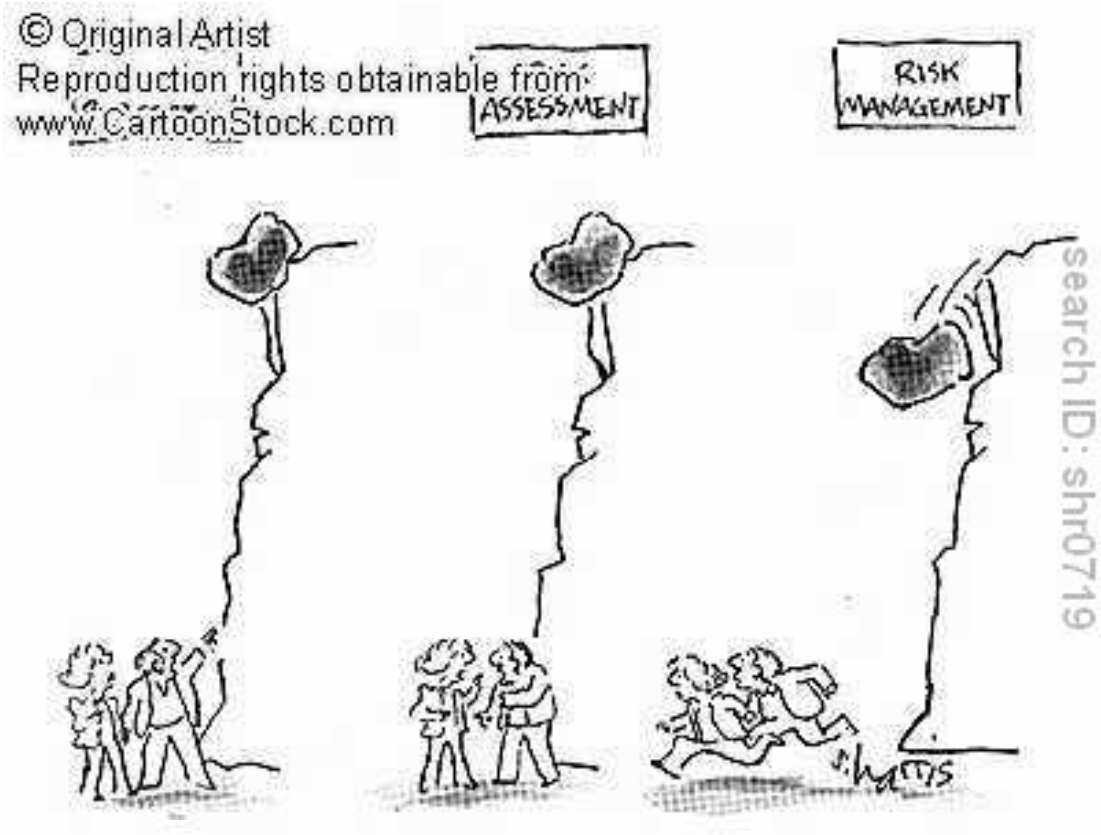
10 características de um CISO

#2 – ASSEGURAR O ALINHAMENTO COM O NEGÓCIO



10 características de um CISO

#3 – REALIZAR UMA GESTÃO EFECTIVA DO RISCO



10 características de um CISO

#4 - ESTAR ATENTO ÀS AMEAÇAS

10 características de um CISO

#5 - TER AS FERRAMENTAS ADEQUADAS

10 características de um CISO

#6 - ESTAR ATENTO À EVOLUÇÃO

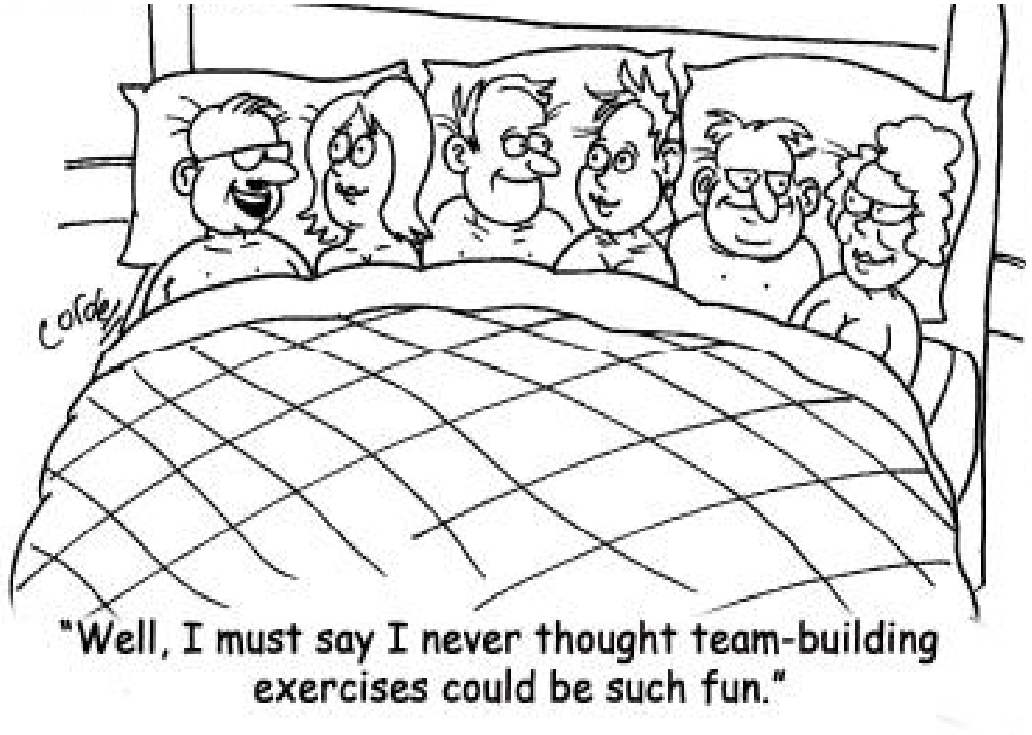
10 características de um CISO

#7 - ACRESCENTAR VALOR

"TREATMENT WITHOUT DIAGNOSIS IS MALPRACTICE."

10 características de um CISO

#8 - FOMENTAR O ESPÍRITO DE EQUIPA



10 características de um CISO

#9 - SER PERSISTENTE

"Why don't you just pick the golfball and take the penalty!"

10 características de um CISO

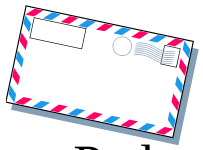
#10 - NEM SEMPRE TEMOS SUCESSO

A Segurança dos Sistemas de Informação

Não é algo que se impõem,

mas sim uma questão de Atitude!

Obrigado



Pedro Cupertino de Miranda

Email: rpmiranda@sonaedistribuicao.pt

Telm: 932441014