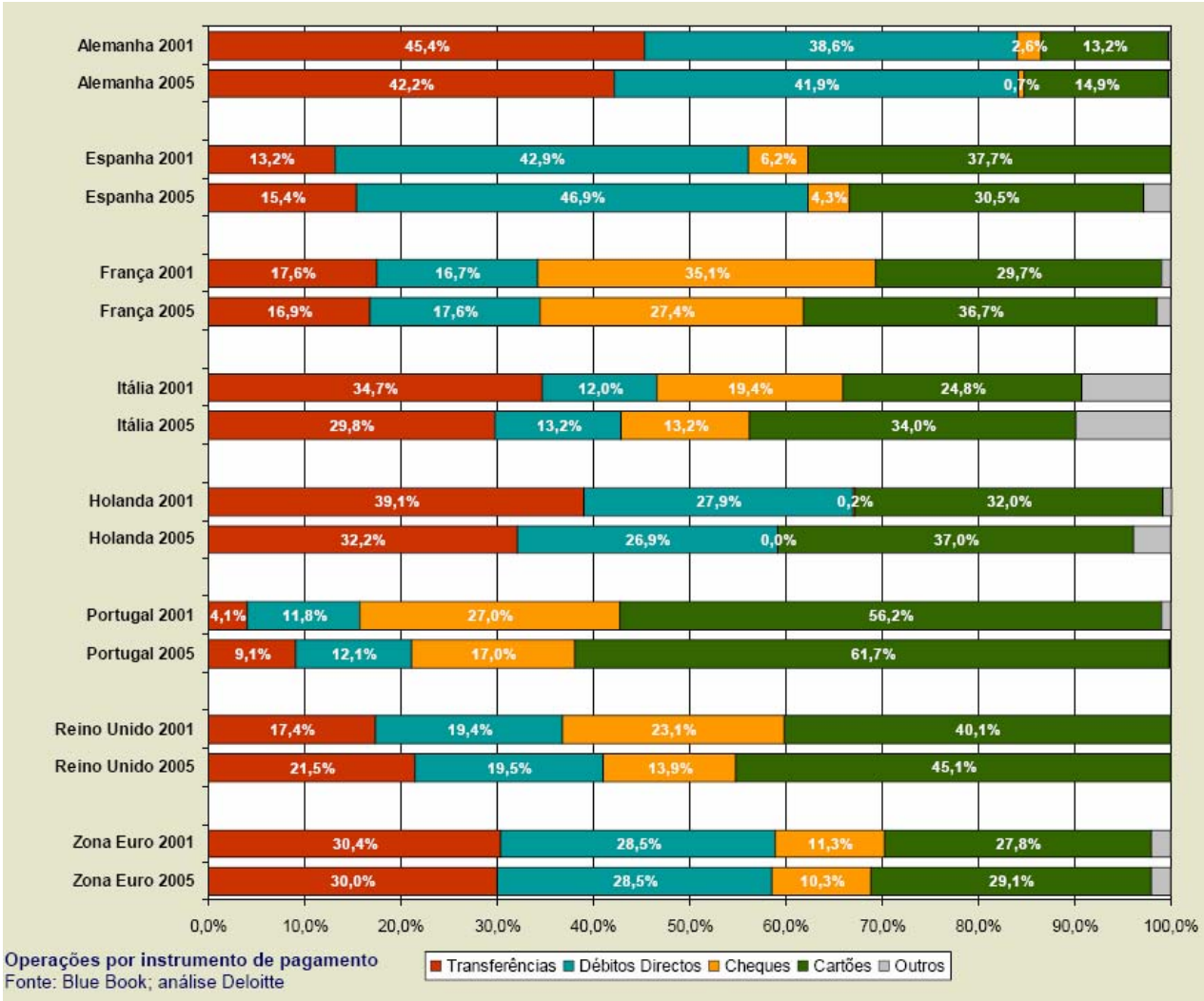

Deloitte.
Trust.
PCI DDS
3 de Abril de 2008
Audit. Tax. Consulting. Corporate Finance.

Meios de pagamento electrónicos têm vindo a ganhar aceitação



Operações por instrumento de pagamento
Fonte: Blue Book; análise Deloitte

- Disparidades na utilização dos instrumentos electrónicos (e.g. Alemanha vs. Reino Unido)
- O cartão é o instrumento que mais cresce na Zona Euro
- Portugal é o País com maior utilização de cartões

O mercado dos cartões de crédito tem vindo a crescer

- Mercado de cartões de crédito em Portugal voltou a crescer em **2007** cerca de **6%,** para um volume de **15,5** mil milhões €
- Actualmente, a UNICRE (maior operador em Portugal) apresentou um crescimento superior da facturação a crédito (cerca de **8%**), relativamente à facturação do débito (4,6%)
- Segundo a UNICRE a fraude no negócio dos cartões em Portugal cresceu ligeiramente (**0,09%**), fixando-se nos **2,9 milhões** € (e.g. Irlanda 11,95 milhões €, Espanha 76,27 milhões €)

Compras a crédito estão a crescer apesar da crise financeira

ANA SUSPIRO

Transacções a crédito atingiram 6,7 mil milhões (
A facturação das compras a crédito cresceu 8%
dados divulgados ontem pela empresa, a crise
nos últimos dois trimestres .

O volume de negócios com cartões de débito t
que a quota das transacções a crédito em Port

A rede Visa gerida pela Unicre movimentou no
do total realizado em Portugal e 15% do consu

O valor médio de cada transacção foi de 36 eu
maior facturação *per capita* no ano passado, d
Portalegre foram os distritos que registaram ma
hotelaria, a expansão de transacções foi da or

No ano de arranque do SEPA (*single european*
internacionalização do mercado de pagamentos
juros transacções acima dos 500 euros para cli
transacções realizadas com cartão para todos os clientes são outros serviços.

Público

ÚLTIMA HORA

Unicre é o 14º maior operador europeu, com 352,8 milhões de transacções

Mercado de cartões de crédito subiu seis por cento em 2007

02.2008 - 12h32 Cristina Ferreira

O mercado dos cartões de crédito em Portugal voltou a crescer em 2007 cerca de seis por cento, para um volume de transacções de 15,5 mil milhões de euros. A empresa portuguesa Unicre cotou-se como o 14º maior operador europeu, com 352,8 milhões de transacções (um milhão de transacções diárias), disse hoje o seu presidente, António Ramalho.

O número de terminais da rede Unicre (POS) cresceu 8,1 por cento, o que coloca a Unicre com uma quota de mercado, à escala portuguesa, de 37 a 40 por cento (nos sistemas terminais).

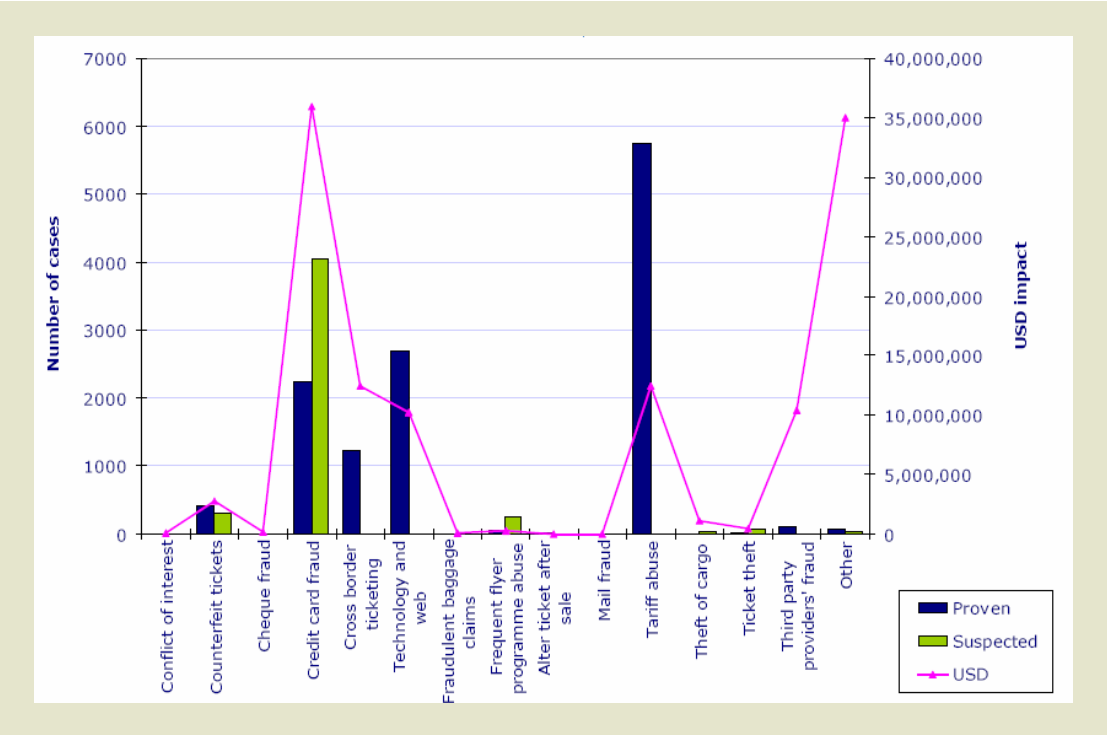
Actualmente, a Unicre detém 215 mil cartões em circulação. A facturação de crédito cresceu mais (cerca de oito por cento) do que a facturação do débito (4,6 por cento). A média europeia de transacções de crédito de curto prazo é de 31 por cento, enquanto em Portugal é de 24 por cento. Em Espanha, essa média atinge 51 por cento.

António Ramalho disse, em conferência de imprensa, que a produção nova da Unicre é praticamente nula, mantendo-se estável em relação a 2006. "Não existe um acréscimo significativo do crédito ao consumo em Portugal. O endividamento é de conveniência [habitação]", disse o gestor.

Em relação à fraude no negócio, "houve um ligeiro acréscimo de 0,09 por cento", para um valor de 2,9 milhões de euros, o que coloca, notou António Ramalho, "Portugal com a menor fraude em toda a Europa". O líder da Unicre observou que na Irlanda (com uma dimensão idêntica à portuguesa) a fraude elevou-se a 11,85 milhões de euros, enquanto em Espanha esse valor atingiu os 76,27 milhões de euros.

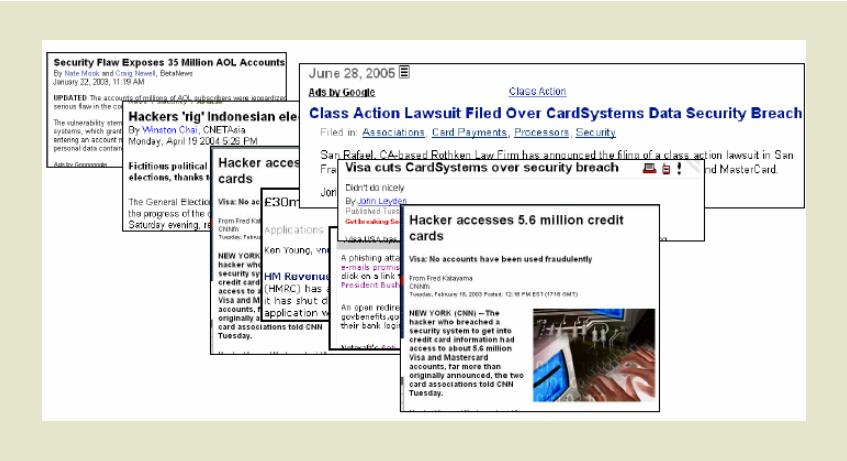
Qual o peso global da fraude com cartões de crédito?

- Resultados do *Global Airline Fraud Survey*, promovido pela Deloitte:
  - Desde 2000 a 2006 a fraude relacionada com cartões de crédito aumentou significativamente, de USD 96k em 2000 para **USD 854k média por companhia em 2006** (na Europa e EUA a média em 2006 por companhia foi de **USD 1,5M)**
  - A fraude relacionada com cartões de crédito é o método de fraude mais comum e dispendioso no sector da aviação



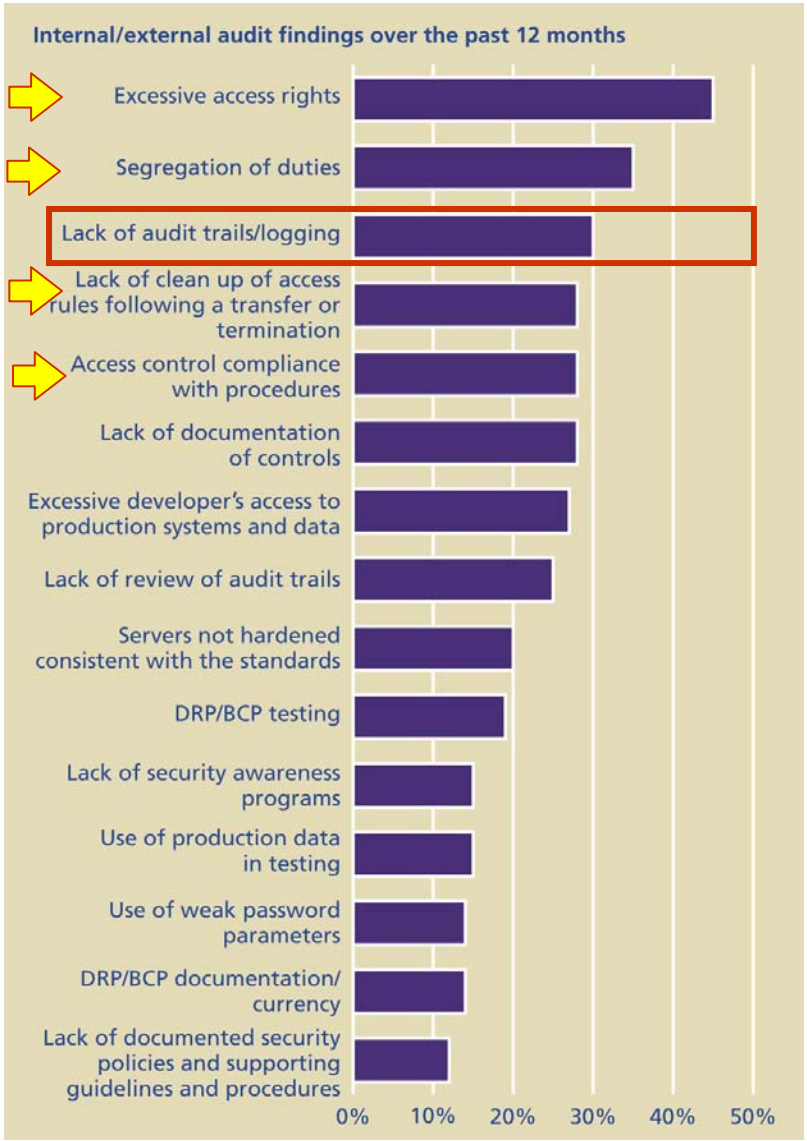
Os impactos por fraude podem ser muito relevantes

- **TJX (TJ Maxx)**: mais de **45 milhões** de números de cartões de crédito e dados pessoais de clientes foram sendo roubados por ***hackers*** durante um período de 18 meses
- **Clonagem organizada**: 13 indivíduos acusados de elaborar operações organizadas de clonagem de cartões de crédito em 40 restaurantes nos EUA, estando o impacto calculado em cerca de **USD 3 milhões**
- **CardSystems**: mais de **40 milhões** de números de cartões de crédito comprometidos. A empresa **abriu falência** em virtude do processo com a Mastercard e do cancelamento dos contratos com a Amex e VISA
- **DSW**: mais de **1,4 milhões** de números de cartões de crédito comprometidos.



Existe a percepção de que, uma parte significa das ocorrências ao nível da segurança decorrer do erro Humano e da tecnologia

- No “Deloitte 2007 *Global Security Survey*” **4** das 5 áreas controlo da segurança, com uma percentagem mais elevada de oportunidade de melhoria/correcção, são relativas à atribuição/manutenção de acessos
- A 5º área de controlo é relativa auditabilidade
- Perante um cenário de fraude poderá ser difícil identificar a causa



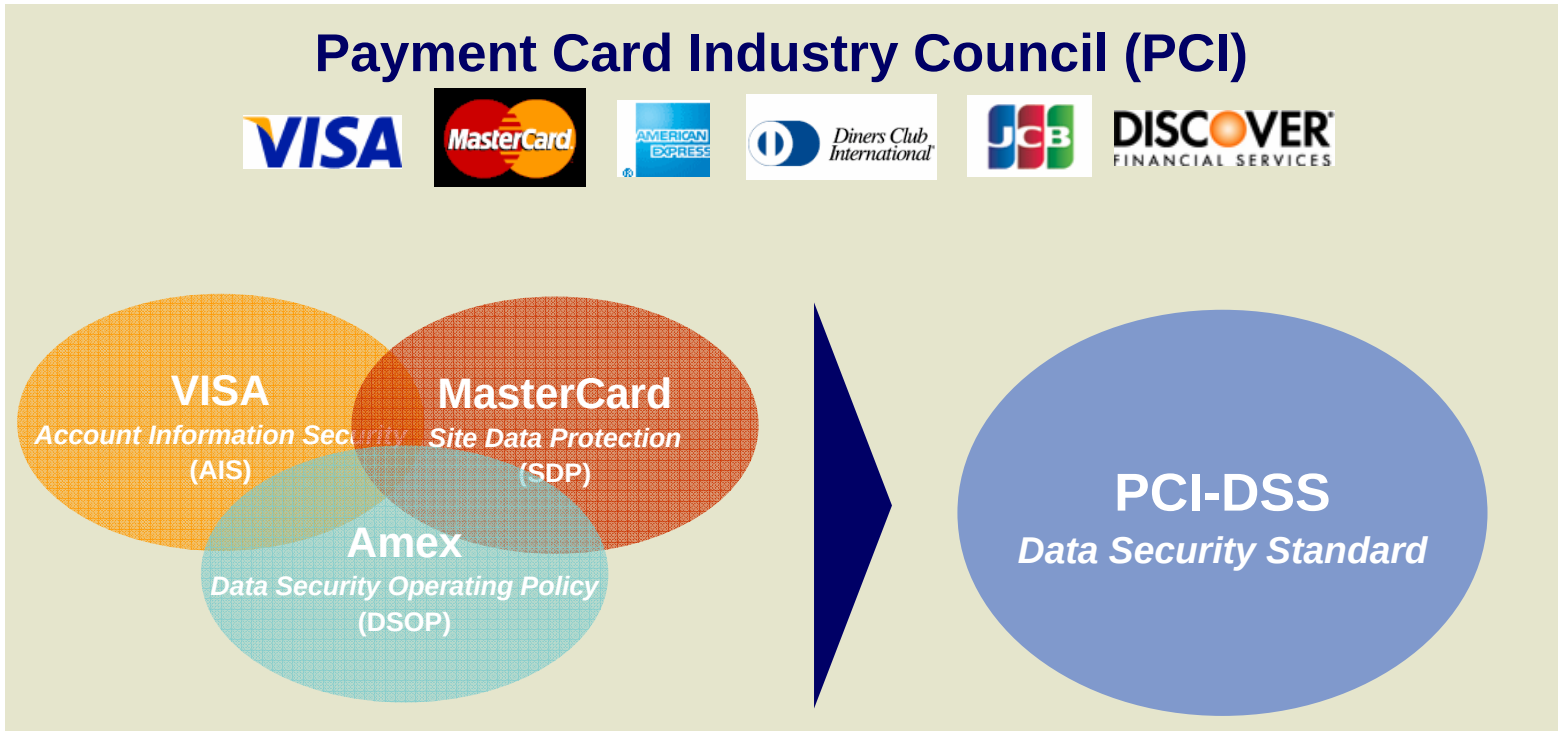
Como identificar uma pessoa fraudulenta?

→ **Existe uma necessidade de controlo**

As ameaças estão em constante transformação, aparecem novos desafios todos os dias

- ***Phishing*** e **ataques** cada vez mais localizados e **sofisticados**
- Crescimento das **ameaças internas**
- Existência de ***gaps*** nos **mecanismos** de **armazenamento,** retenção e encriptação de dados
- **Riscos** de segurança associados às **tecnologias *wireless***
- Aumento dos ***worms*** nas **redes empresariais**

Necessidade de criar um *standard* comum que estabeleça as boas práticas de segurança (PCI - *Data Security Standar)*



O principal objectivo do *Payment Card Industry/Data Security Standard* (PCI/DSS) é reduzir drasticamente fraudes

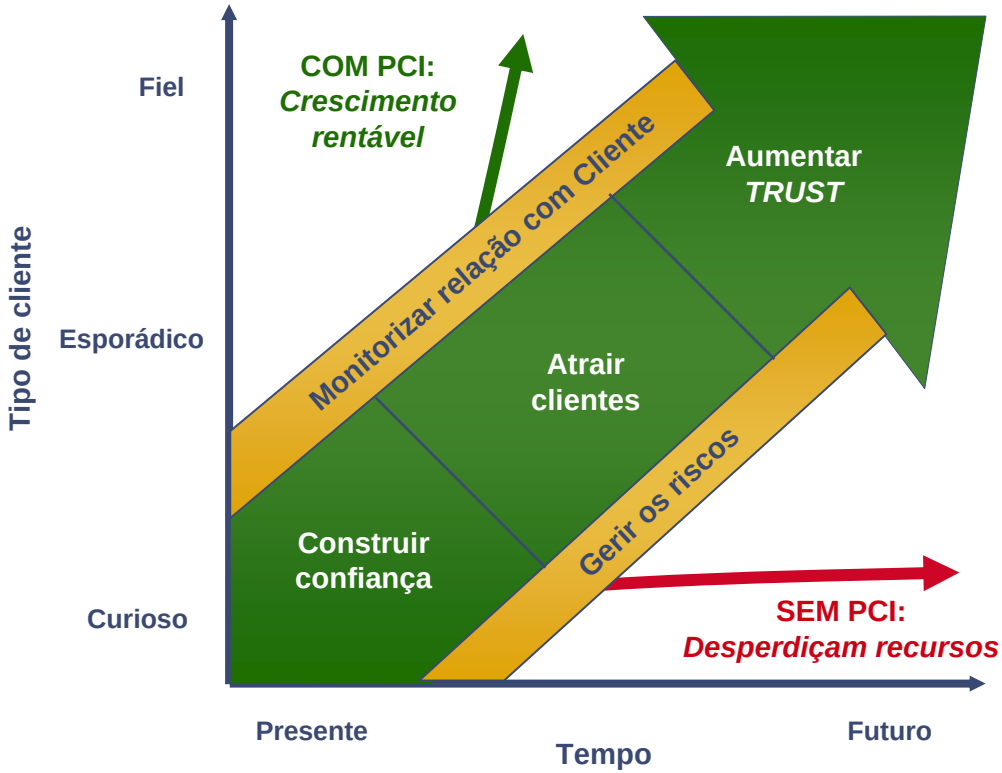
- É necessário **assegurar** que todos os Membros (Emissores e Adquirentes), Agentes, Comércio e Prestadores de Serviços que **armazenam, processam e/ou transmitem dados e transacções** dos portadores de cartão estejam **alinhados** com o PCI/DSS.
- O **cumprimento** do **PCI/DSS** é uma **obrigação** de todas as entidades que **processam, transmitem** ou **armazenam** informações/transacções dos Portadores de Cartão.
- As **operadoras de cartão de crédito** e os **bancos emissores** são **responsáveis** por **contactar** o **comércio**, os ***gateways*** de pagamento e os **prestadores de serviço** para **informar** sobre seus **requisitos** e **prazos**
- Nos casos em que a **organização demonstre** a sua conformidade com o PCI/DSS, por meio de relatório **auditoria anual** (realizado pelo *Qualified Security Assessor* – QSA), dos relatórios de **testes de vulnerabilidade** periódicos (conduzidos pelo *Approved Scanning Vendor* – ASV) e por fim, não tenha recebido **chamadas de atenção** na análise forense (realizada pelas marcas), quando ocorra um incidente, **não estará sujeita às penalidades e não será considerada responsável.**

Nem todas as áreas e requisitos do PCI DSS apresentam o mesmo grau de maturidade

Requisitos PCI	*Compliance Benchmark*
Build and Maintain a Secure Network	
1 – install and maintain a firewall configuration to protect data	53%
2 – do not use vendor supplied defaults for system passwords and other security parameters	16%
Protect Cardholder Data	
3 – Protect stored data	21%
4 – Encrypt transmission of cardholder data and sensitive information across public networks	22%
Maintain a Vulnerability Management Program	
5 – use and regularly update anti-virus software	50%
6 – Develop and maintain secure systems and applications	37%
Implement Strong Access Control Measures	
7 – Restrict access to data by business need-to-know	50%
8 – Assign a unique ID to each person with computer access	45%
9 – Restrict physical access to cardholder data	48%
Regularly Monitor and Test Networks	
10 – Track and monitor all access to network resources and cardholder data	46%
11 – Regularly test security systems and processes	16%
Maintain an Information Security Policy	
12 – Maintain a policy that addresses information security	48%

A Proposição de Valor do PCI/DSS

- Estabelecer ***framework* comum** de Segurança da Informação.
- Demonstrar transparência, confiança (TRUST), seriedade e coesão nas ações de segurança de informação.

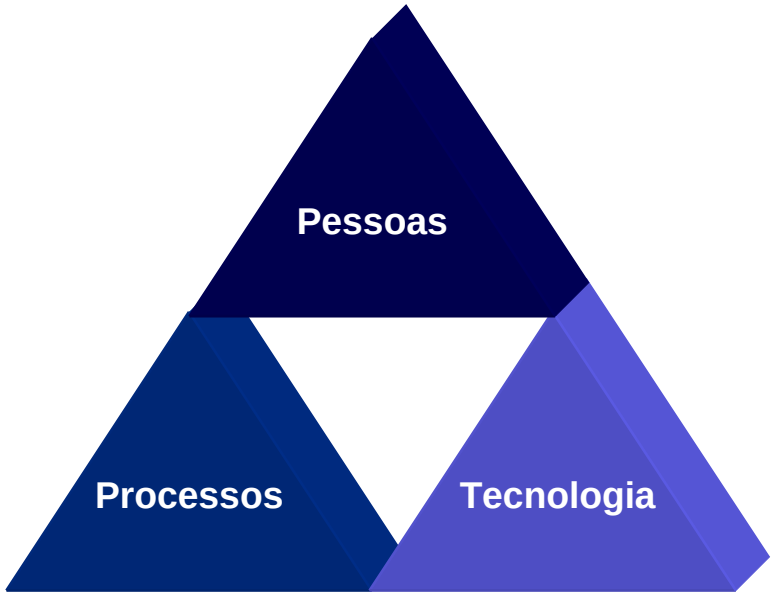


- Antecipar e gerir **riscos** e impactos (financeiros, operacionais e de imagem).
- Promover a **integridade** do *Brand* e aumentar a **confiança** de seus consumidores nos meios de pagamento de cartão de crédito.

A Visão da Deloitte sobre os requisitos do PCI/DSS

Objetivos da Segurança da Informação

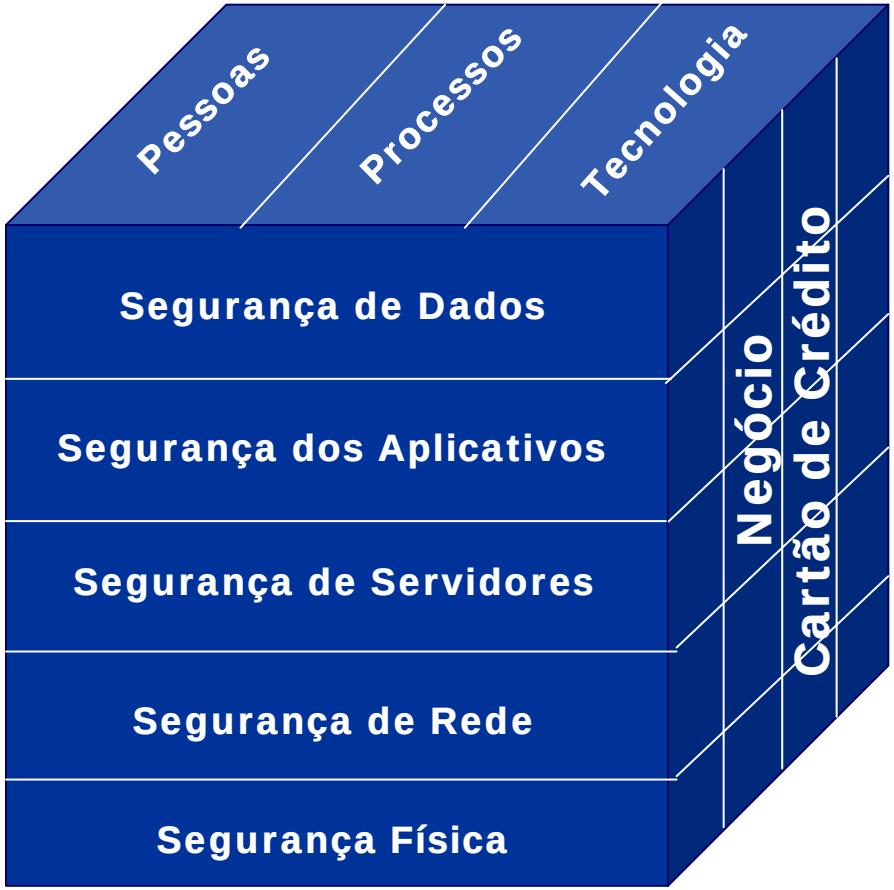
Controlos de Segurança da Informação



Objetivos de Segurança da Informação & *PCI/DSS*

- Os **objetivos e *guidelines*** do PCI/DSS potencias as **diversas camadas** de **segurança da informação**, desde a segurança **física** até a segurança dos **dados**, passando pela segurança de **rede**, dos **servidores** e das **aplicações**

- **Cada** uma destas **camadas** é por sua vez subdividida em diversos **controlos de segurança** que potenciam as **pessoas**, os **processos** e as **tecnologia** de suporte às operações com cartão de crédito



A nossa abordagem adopta as *guidelines* da PCI DSS e tem em consideração as *lessons learn* apreendidas

- Qualified Security Assessors (QSAs)
- Approved Scanning Vendors (ASVs)

Contacto

Miguel Barão da Cunha

micunha@deloitte.pt

Deloitte.

Lisboa

Edifício Atrium Saldanha
Praça Duque de Saldanha, 1 - 6º
1050-094 Lisboa
Portugal
Tel: +(351) 210 422 500
Fax: +(351) 210 422 950

Porto

Bom Sucesso Trade Center
Praça do Bom Sucesso, 61 - 13º
4150-146 Porto
Portugal
Tel: +(351) 225 439 200
Fax: +(351) 225 439 650

Luanda

Rua Engº Costa Serrão, nº 13
Luanda
República de Angola
Tel: +(244) 222 391 808 / 391 673
Fax: +(244) 222 391 972