Técnicas e ferramentas de investigação da fraude

PEDRO CUPERTINO DE MIRANDA
CISA, CISM

ISCAC, 19 de Junho de 2010

Factos Relevantes 2009

Líder no retalho
em Portugal (alimentar e não alimentar)
Presença em Espanha

Mais de 4,2 Bn€
Vendas (215.000 artigos no portfolio)

~35.000
empregados (maior empregador privado em Portugal)

809.000
Área de venda
(em 793 lojas)

~3.500
fornecedores

~3 M€
Clientes/semana (talões de venda)

2

Portfolio de Negócios

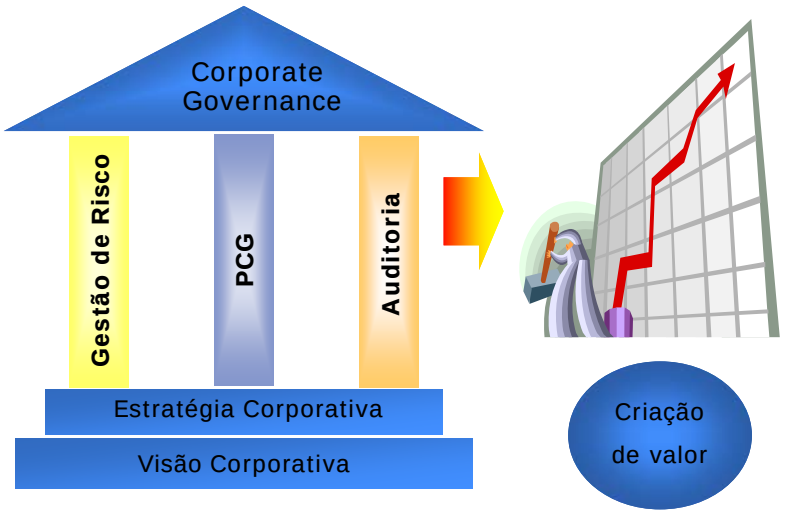
3

Missão da Direcção de Auditoria e Gestão de Risco

Contribuir de forma efectiva na concretização dos objectivos da organização, através de uma actuação sistemática e metódica na avaliação e gestão dos principais riscos e controlos dos processos de negócio.

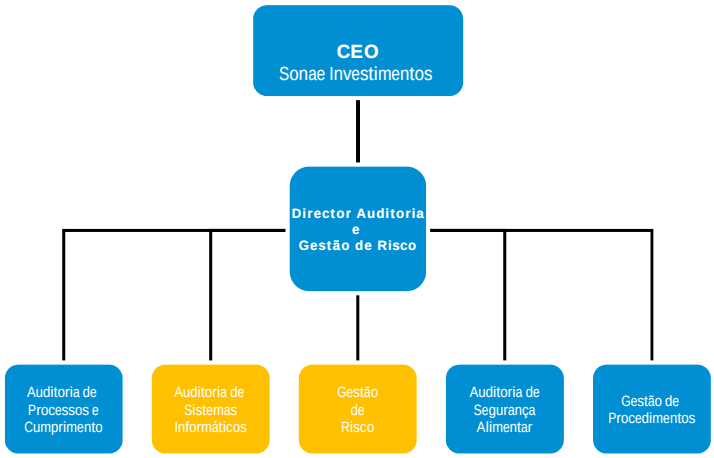
4

Corporate Governance



5

Como estamos Organizados



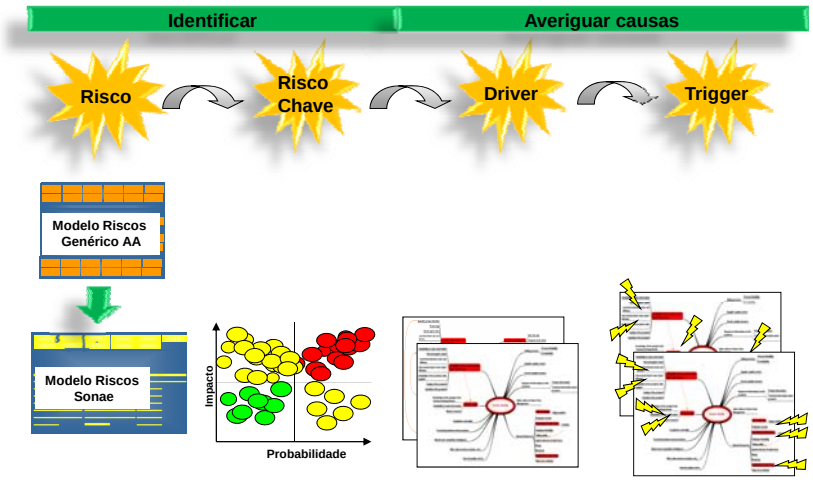
Nr de colaboradores: 37

6

Auditoria baseada no Risco

ISCAC, 19 de Junho de 2010

O processo de Gestão de Risco

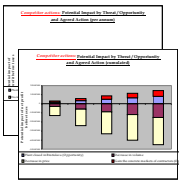


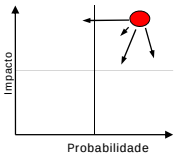
8

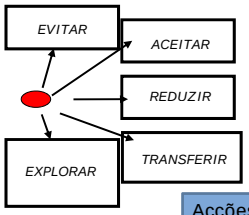
O processo de Gestão de Risco

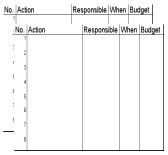
Medir | Avaliar | Gerir

Indicadores Performance → Indicadores Risco → Opções → Acções









Indicadores Leading
Indicadores Lagging

Indicadores de Risco

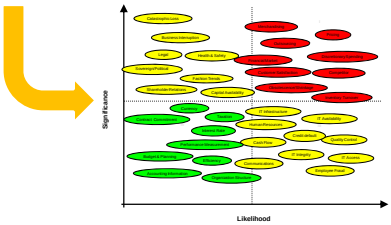
Acções para:
- Gerir o risco
- Melhorar indicadores
- Melhorar a Gestão Risco
- Acções imediatas

9

O processo de Gestão de Risco

Modelo de Riscos Genérico

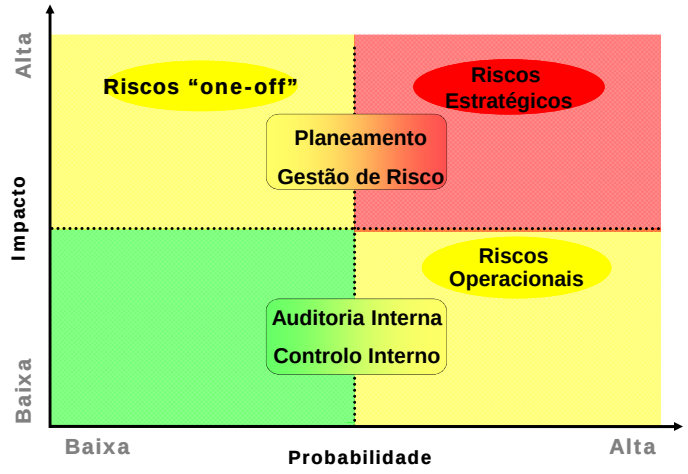
A classificação dos riscos do BRM nas dimensões Impacto e Probabilidade de Ocorrência, deu origem à sua prioritização no mapa de riscos.



Mapa de Riscos da Sonae

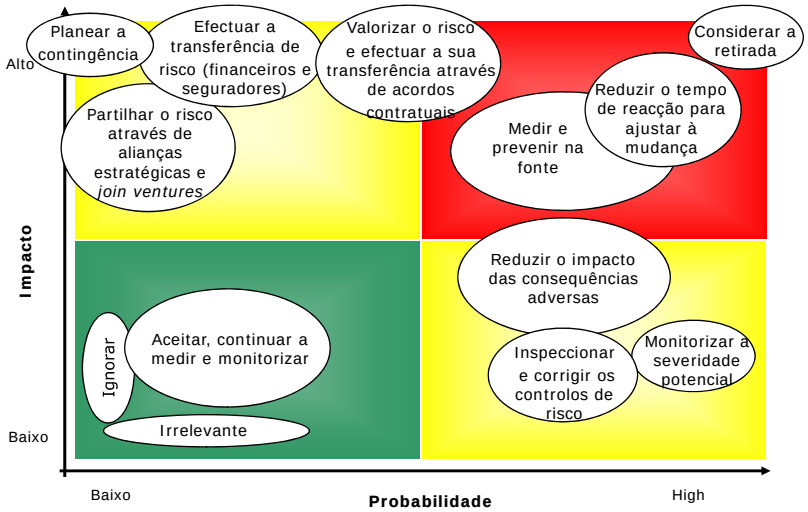
10

Auditoria e a Gestão de Risco



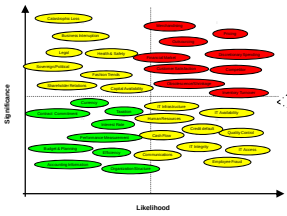
11

Atitude face ao Risco



12

Plano de actividade



Programa de trabalho Auditoria

Plano de Gestão de Risco

O plano de actividades da Auditoria e da Gestão de Risco é baseado nos resultados do processo periódico de avaliação de risco da Empresa e consistente com os seus objectivos.

13

Fraude

ISCAC, 19 de Junho de 2010

Formas de Fraude

Num sentido amplo, uma **fraude** é um esquema criado para obter ganhos pessoais

– Roubo, desfalque
– Falsas declarações (documentos financeiros, empréstimos, aplicações)
– Corrupção, conluio, subornos
– Apropriação não autorizada de activos e bens (despesas de viagem, salários, equipamentos, produtos)
- Roubo de identidade

15

Por que é que se comete fraude?

Necessidade > Medo = Fraude

A equação da Fraude!

16

Evolução da Fraude

Factores que contribuem para o aumento da Fraude

1. Inexistência de standards e regras de conduta
2. Controlos inadequados
3. Não se aposta na prevenção
4. Enfraquecimento dos Valores da sociedade
5. Existência de ferramentas e técnicas mais sofisticadas
6. Redução do número de colaboradores

7. Pressões económicas

17

Razões para se cometer fraude

Porquê é que se comete Fraude?

- Necessidade de dinheiro (“desespero”)
- Frustração/desmotivação no trabalho
- Problemas pessoais
- Síndroma de Toda-A-Gente-O-Faz
- Gozo pessoal “Vencer o Sistema”
- O sistema de controlo interno é fraco
- Baixa probabilidade de detecção
- Baixa probabilidade de ser acusado/condenado

18

O triângulo da Fraude

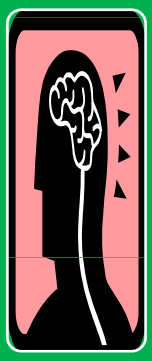
Incentivo

- Problemas financeiros
- Hábitos e comportamentos de risco
- Relacionado com o trabalho
- Desejo de sucesso / ambição

19

O triângulo da Fraude

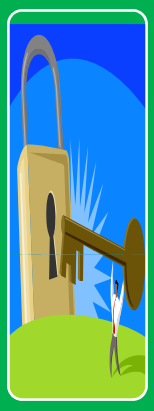
Racionalização



- O perpetrador convence-se que o que faz é moralmente justificável
- "Assim que puder pago"
- "Sinto-me que estou mal pago"
- "Trabalho mais do que os outros"
- Frustração como consequência de promoções e aumentos que não se concretizaram

20

O triângulo da Fraude

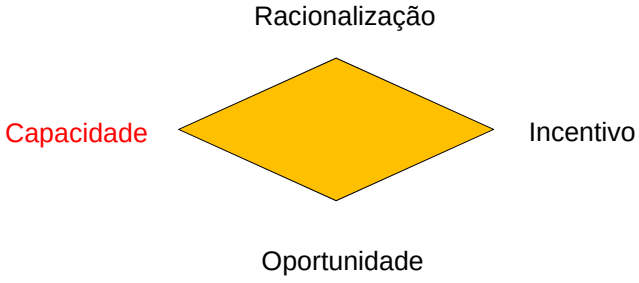


Oportunidade

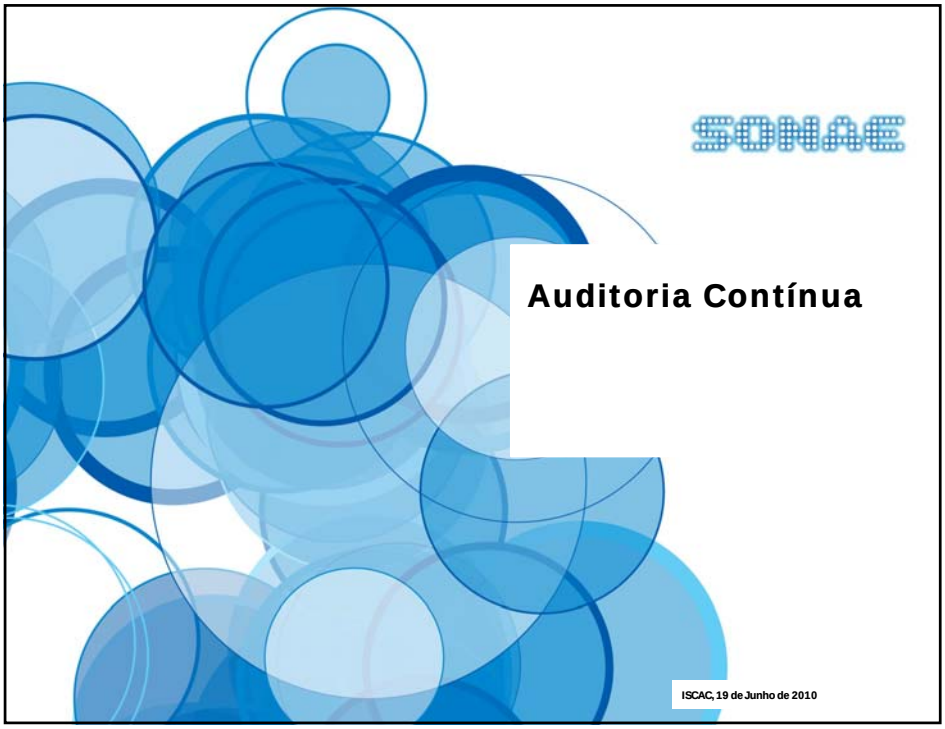
- Controlos internos fracos ou inexistentes
- Inexistência de segregação de funções
- Organização altamente descentralizada
- Falta de conhecimento ou de sensibilidade para o tema da Fraude

21

O triângulo da Fraude estendido



22



Evolução da Quebra no Retalho

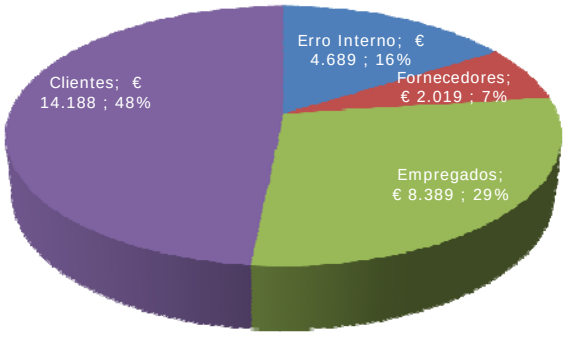
	Total de Quebra (€ milhões)	Quebra 2007 (% turnover)	Quebra 2007 (% turnover)	Percentagem Variação 2006-2007
Austria	432	0.94	0.96	-2.1%
Belgica	812	1.33	1.28	3.9%
Dinamarca	367	1.2	1.24	-3.2%
Finlandia	416	1.32	1.34	-1.5%
França	4,645	1.34	1.29	3.9%
Alemanha	4,906	1.1	1.07	-2.8%
Grécia	523	1.36	1.33	2.3%
Islândia	27	1	1.06	-5.7%
Irlanda	438	1.33	1.25	6.4%
Itália	3,085	1.23	1.24	-0.8%
Holanda	1,180	1.24	1.2	3.3%
Noruega	431	1.26	1.29	-2.3%
Portugal	359	1.31	1.34	-2.2%
Espanha	2,645	1.28	1.29	-0.8%
Suécia	632	1.32	1.32	0.0%
Suiça	587	0.96	0.92	4.3%
Inglaterra	5,596	1.34	1.33	0.8%
Europa de Leste	**27,081**	**1.25**	**1.23**	**1.6%**
República Checa	360	1.41	1.42	-0.7%
Hungria	336	1.36	1.38	-1.4%
Polónia	1,172	1.34	1.32	1.5%
Eslováquia	129	1.36	1.4	-2.9%
Estados Bálticos	207	0.142	1.32	7.6%
Europa Central	**2,204**	**1.36**	**1.35**	**1.0%**
Europa de Central e de Leste	**29,285**	**1.26**	**1.24**	**1.6%**
Mundial	**72,424**	**1.36**	**1.34**	**1.5%**

Fonte: Global Retail Theft Barometer 2007

24

Origem da Quebra

Quebra no Retalho na Europa (milhões de €)

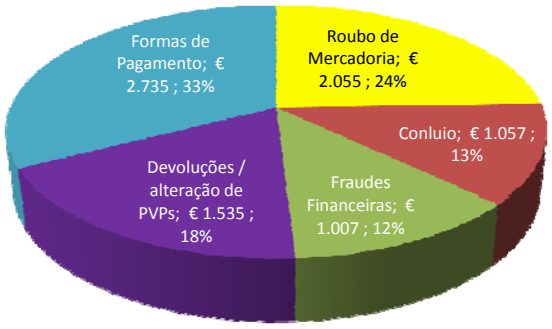


Fonte: Global Retail Theft Barometer 2007

25

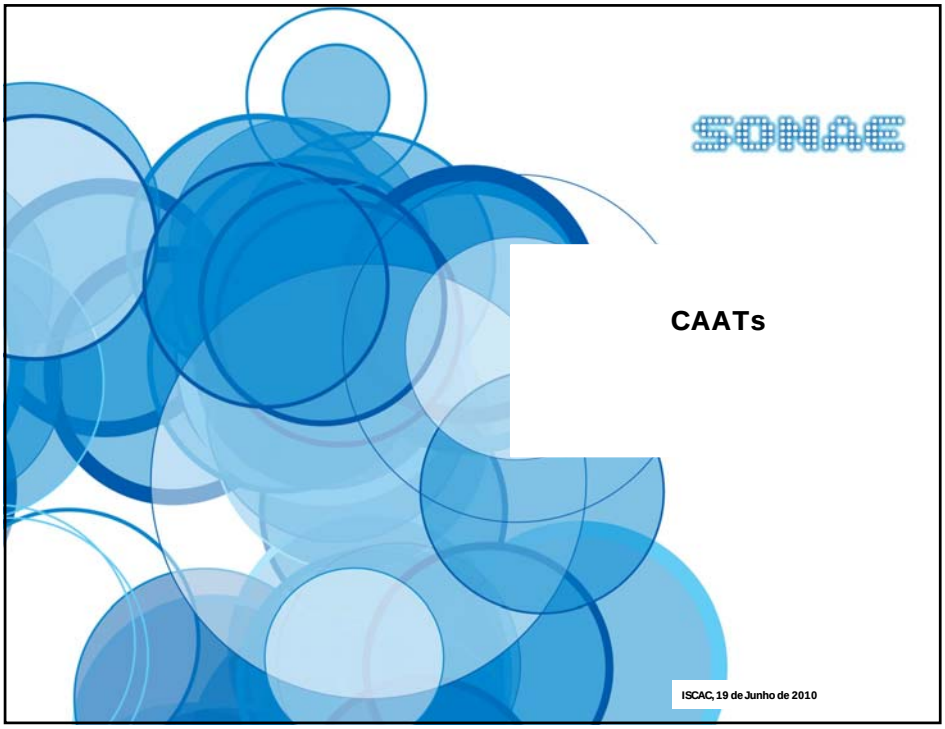
Métodos de Roubo Interno

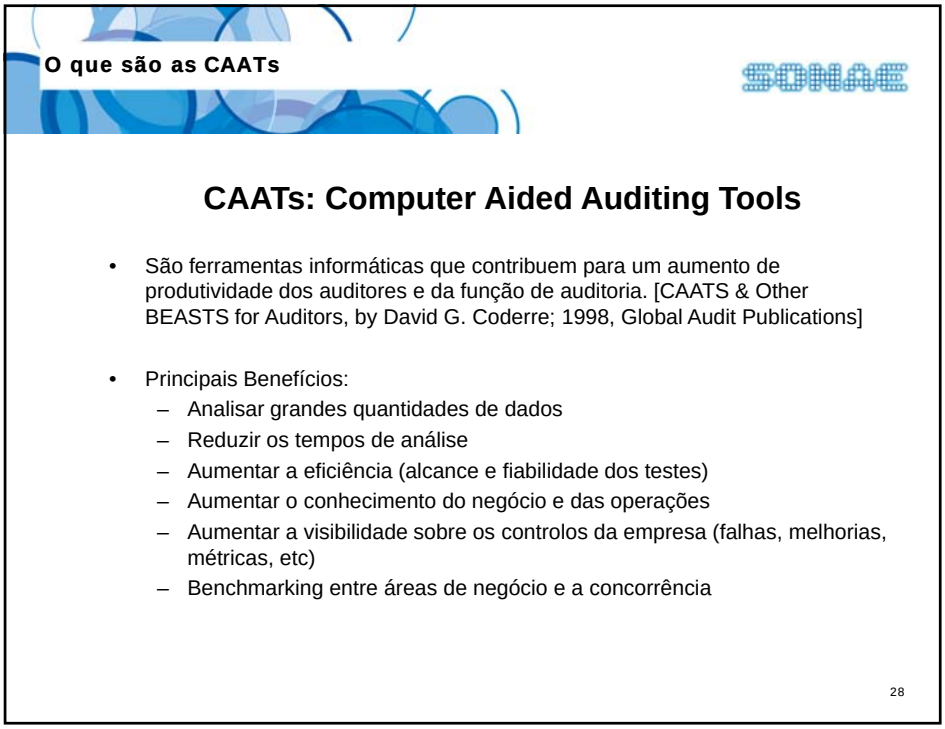
Roubo Interno na Europa 2007 (milhões de €)



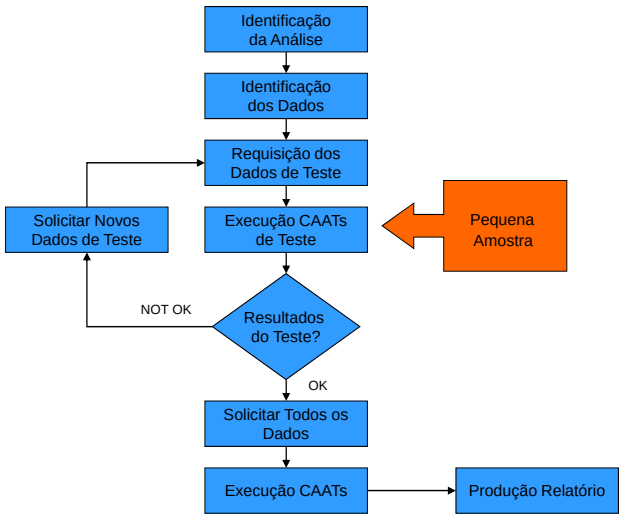
Fonte: Global Retail Theft Barometer 2007

26


SONAE
CAATs
ISCAC, 19 de Junho de 2010


O que são as CAATs
SONAE
CAATs: Computer Aided Auditing Tools
• São ferramentas informáticas que contribuem para um aumento de produtividade dos auditores e da função de auditoria. [CAATS & Other BEASTS for Auditors, by David G. Coderre; 1998, Global Audit Publications]
• Principais Benefícios:
– Analisar grandes quantidades de dados
– Reduzir os tempos de análise
– Aumentar a eficiência (alcance e fiabilidade dos testes)
– Aumentar o conhecimento do negócio e das operações
– Aumentar a visibilidade sobre os controlos da empresa (falhas, melhorias, métricas, etc)
– Benchmarking entre áreas de negócio e a concorrência
28

Fluxograma de Análise de Dados



29

Como controlar os resultados das CAATs

- O auditor deve assegurar que não existe manipulação de dados através de:
  - Participação no desenho e no teste dos programas
  - Verificação do código por forma a assegurar que este se encontra conforme as especificações
  - Aprovação das especificações técnicas e da realização de revisões periódicas aos trabalhos executados pelas ferramentas
  - Revisão dos controlos informáticos que possam comprometer a integridade das ferramentas e dos respectivos resultados.
  - Integração automática dos resultados no processo de auditoria
- O auditor deve validar o software de auditoria através da utilização de um conjunto reduzido de dados de teste antes de se poder utilizar dados de produção.
- O auditor deve garantir a protecção dos dados através da implementação de mecanismos de controlo de acesso.

30

Software para análise de dados

- Microsoft Access e Excel
- Interactive Data Extraction And Analysis (IDEA)
- Audit Command Language (ACL)

- Características adicionais que o software deverá ter:
  - Baseado em produtos Windows e de fácil utilização
  - Necessita de criatividade e de imaginação
  - E de muita massa cinzenta

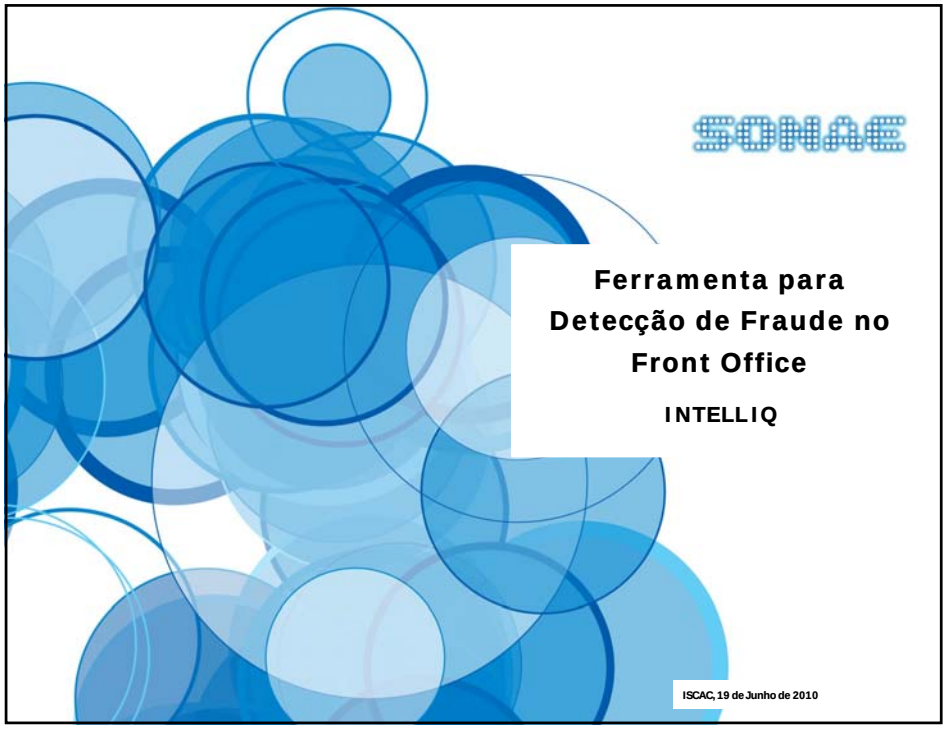
31

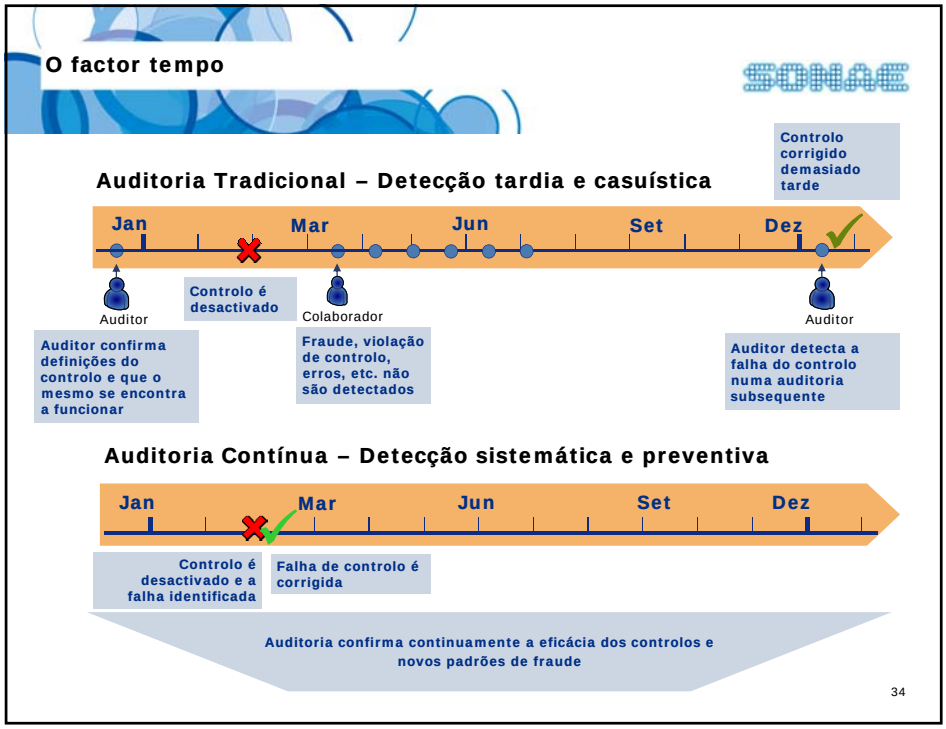
Ferramentas de Análise de Dados

Tools	Capacity	Ease of use	Analytic Capabilities
Microsoft Excel	• 65,536 rows by 256 columns • 255 chars per field	• Standard, easy to use office application	• Data analysis toolkit • Built-in functions
Microsoft Access	• 2 GB database • 255 fields (columns)	• Training is required	• Built in functions • Great for joining tables
ACL	• Unlimited	• Requires basic training • Menu based	• Complete set of preprogrammed analysis
Monarch	• 1,000,000 input pages	• Training is required	• Provides basic analytic capabilities
Microsoft SQL Server	• 1,048,516 terabytes • 1,024 columns	• Advanced training required	• Built in functions • Great for joining tables

Excellent Good Satisfactory Poor Very poor

32

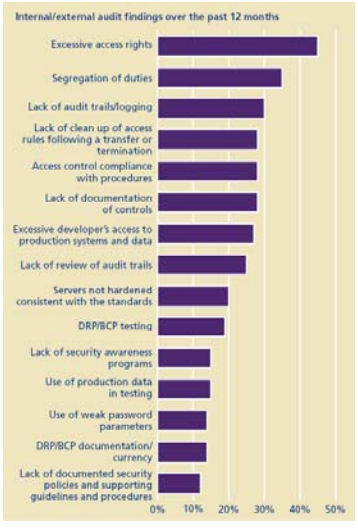

SONAE
Ferramenta para Detecção de Fraude no Front Office
INTELLIQ
ISCAC, 19 de Junho de 2010


O factor tempo
SONAE
Auditoria Tradicional – Detecção tardia e casuística
Controlo corrigido demasiado tarde
Jan
Mar
Jun
Set
Dez
Auditor
Controlo é desactivado
Colaborador
Auditor
Auditor confirma definições do controlo e que o mesmo se encontra a funcionar
Fraude, violação de controlo, erros, etc. não são detectados
Auditor detecta a falha do controlo numa auditoria subsequente
Auditoria Contínua – Detecção sistemática e preventiva
Jan
Mar
Jun
Set
Dez
Controlo é desactivado e a falha identificada
Falha de controlo é corrigida
Auditoria confirma continuamente a eficácia dos controlos e novos padrões de fraude
34

A actividade de Auditoria de Sistemas

ISCAC, 19 de Junho de 2010

Principais Riscos IT



Deloitte.

2007 Global Security Survey

The shifting security paradigm

Principais áreas de Preocupação

- Excessivos direitos de acesso;
- Segregação de funções;
- Falhas no processo de transferência ou cessação de funções;
- Monitorização dos registos de Auditoria

36

O caso do Société Générale


Diário de Notícias

Edições Anteri
Quinta, 7 de Fevereir
Edição Papel

Lisboa 01.02.08 dn.homepage » dn.bolsa

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

Controles 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 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.

37

O caso da AMD

O caso da AMD

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*.

38

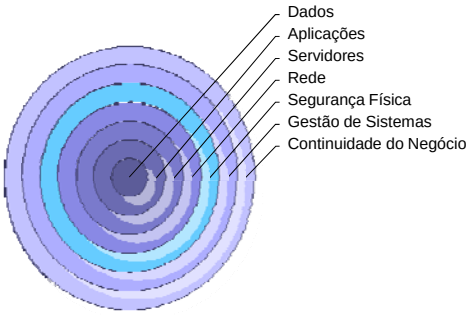
Outros exemplos de fraude

- Roubo de informação sobre mais de 45.6 milhões de cartões de crédito/débito no retalhista T.J. Max
- Roubo de um disco que continha dados pessoais relativos a mais de 25 milhões de cidadãos ingleses.
- Roubo de portátil que continha dados pessoais relativos a mais de 26 milhões de veteranos de guerra americanos
- Sites governamentais da Estónia são alvo de ciber ataques oriundos da Rússia
- Hacker explora falha de segurança e tem acesso a informação sobre mais de 100 contas de emails utilizadas por várias embaixadas.

39

CAATs

As CAATs também podem ser aplicadas às Auditorias Informáticas



40

Auditoria a Aplicações

Exemplos de Ferramentas para Auditoria de Aplicações

Tipo	Descrição	Exemplos
Password Crackers	Ferramenta utilizada na revelação de passwords (dicionário ou brute force)	• Lophcrack • Cain&Abel • LC4 • John the Ripper
Scanners de Vulnerabilidades	Ferramenta utilizada na identificação de falhas associadas a cross site scripting, buffer overflow, SQL injection, broken authentication	• WebInspect • Brutus • Nikto • SpikeProxyLite
Recolha de conteúdos WEB	Ferramenta utilizada na recolha de conteúdos de páginas WEB (HTTP, HTTPS, ASP) permitindo a sua análise em modo offline	• WGet • HTTPpush • WFetch • WhiteHat

41

Auditoria de Base de Dados

Exemplos de Ferramentas para Auditoria de Base de Dados

Tipo	Descrição	Exemplos
Password Crackers	Ferramenta utilizada na revelação de passwords (dicionário ou brute force)	• Appdetective • ISS Database Security • OAT • SQLAT
Scanners de Vulnerabilidades	Ferramenta utilizada na identificação de falhas associadas a versões e nível de patching, buffer overflow, utilizadores, perfis e passwords e erros de configuração	• Appdetective • ISS Database Security • OAT • SQLAT

42

Auditoria a Servidores

Exemplos de Ferramentas para Auditoria de Servidores

Tipo	Descrição	Exemplos
Password Crackers	Ferramenta utilizada na revelação de passwords (dicionário ou brute force)	• LC4 • John The Ripper • MD5 Crack • Brutus
Scanners de Vulnerabilidades	Ferramenta utilizada na identificação de falhas associadas a versões e nível de patching, buffer overflow, utilizadores, perfis e passwords e erros de configuração	• Nessus • ISS Host Scanner • Languard • Retina
Utilities	Ferramentas para análise de configurações que também podem ser utilizadas em ataques mais cirúrgicos	• PSExec • NFSShell • Windows Administration Tool Pack • Dump (users, evt, reg, sec)

43

Auditoria às Redes

Exemplos de Ferramentas para Auditoria da Rede

Tipo	Descrição	Exemplos
Sniffers	Ferramenta utilizada na captura de tráfego que circula na rede	• SnifferPro • Snort • EtherReal • DSniff
Scanners	Ferramenta utilizada na identificação serviços de rede activos e respectiva exploração de vulnerabilidades	• ISS Network Scanner • Nmap • NBTScan • Qualys
Utilities	Ferramentas para análise de configurações que também podem ser utilizadas em ataques mais cirúrgicos	• SamSpade • SolarWinds • SNMP Scan • Fping

44

Auditoria da Rede Wireless

Exemplos de Ferramentas para Auditoria da Rede Wireless

Tipo	Descrição	Exemplos
Wireless	Ferramentas utilizadas na descoberta de redes wireless e posterior ataque aos métodos de autenticação	• Netstumbler • AirSnort • Kismet • WLanMeter

45

Conclusões finais

Factores críticos de sucesso para uma detecção efectiva da Fraude:

- Começar por identificar os Riscos
- Implementar controlos internos fortes
- Monitorizar de forma contínua as áreas de risco
- Formar colaboradores com o know-how necessário
- Possuir Ferramentas adequadas
- Acreditar que nos pode acontecer

46

Perguntas e Respostas

SONAE

OBRIGADO

47

Nome da Apresentação/
SUBTÍTULO

SONAE

Pedro Cupertino de Miranda

RPMIRANDA@SONAE.PT

ISCAC, 19 de Junho de 2010

48