


- Agenda**
- Governança
 - Padrões
 - Processos e TI
 - Intervalo / Networking
 - Governança em TI - COBIT ITIL e demais padrões
 - Questões
 - Sorteio: Vagas nos cursos




Mas, enfim...o que realmente é


"GOVERNANÇA"

??

4


O que é GOVERNANÇA
Muitas definições...





5

O que é GOVERNANÇA
Muitas definições...



BOVESPA - Bolsa de Valores de São Paulo:

Governança Corporativa é o sistema que permite aos acionistas ou cotistas e governo estratégico de sua empresa e a efetiva monitoração da direção executiva.

As ferramentas que garantem o controle da propriedade sobre a gestão são o Conselho de Administração, a Auditoria Independente e o Conselho Fiscal.

BRASIL

6

O que é GOVERNANÇA
Muitas definições...




Sarbanes Oxley: Sarbanes-Oxley Act aims to raise standards of corporate governance and obliges company directors to take direct responsibility for the reliability of their firms' accounts.


IOG (Institute on Governance), Canadá:
"the art of steering societies and organizations."

7

IBCG – Instituto Brasileiro de Governança Corporativa




Governança corporativa é o sistema pelo qual as sociedades são dirigidas e monitoradas, envolvendo os relacionamentos entre Acionistas/Cotistas, Conselho de Administração, Diretoria, Auditoria Independente e Conselho Fiscal. As boas práticas de governança corporativa têm a finalidade de aumentar o valor da sociedade, facilitar seu acesso ao capital e contribuir para a sua perenidade.



8


O que é GOVERNANÇA
Muitas definições...



World Bank: Conceptually, governance (as opposed to "good" governance) can be defined as the rule of the rulers, typically within a given set of rules. One might conclude that governance is the *process* – by which authority is conferred on rulers, by which they make the rules, and by which those rules are enforced and modified.

SDT-OGC (Office Of Government Commerce), UK:
Governance is concerned with accountability and responsibilities; it describes how the organisation is directed and controlled.

9

OGC – UK Government / ITSM
 Dos conceitos às praticas... 

"Governance is the framework within which strategy is formally managed, including such elements as reporting arrangements, roles and responsibilities, policies and standards, and risk management"
 (In "Business and IT Strategies" – ITSM/OGC – UK Government)

A GOVERNANÇA é a estrutura escolhida para permitir o gerenciamento formal da estratégia e inclui todos os elementos que suportam tal gerenciamento, tais como os relatórios, responsabilidades e atribuições, políticas e padrões e o gerenciamento de riscos.

10

Da visão de negócios à operação
 O desafio de alinhar visão ,estratégia e operação 

Para onde vamos?

Como nós podemos chegar lá?

O que precisamos fazer BEM FEITO ?

Como suportamos as operações diárias?



Vision statement

↓

Strategy map


↓

Targets

↓

Action


11

Há um único modelo de GOVERNANÇA ?
 A Governança relaciona-se aos objetivos maiores da empresa. 

Quais são os objetivos maiores de uma empresa ?
 Há diferentes escolas e diferentes direcionadores. Como exemplo:

<i>Escola Americana</i>	<i>Valor para o Acionistas</i>
<i>Escola Européia</i>	<i>Valor para Stakeholders (clientes, colaboradores, acionistas, fornecedores)</i>
<i>Escola Japonesa</i>	<i>Harmonia Social (benefício social, longo prazo)</i>
<i>Escola ...</i>	<i>Ênfase em ...</i>

12 Baseado em: Peter Drucker – Desafios Gerenciais para o Século XXI


Porquê a GOVERNANÇA ?
 Necessidade de **CONTROLE** e **VISIBILIDADE**. 

CONTROLE para atuar de forma eficaz sobre o curso da empresa, alinhando ações e prioridades com os direcionadores estratégicos.

**** Processos de tomada de decisões ****

VISIBILIDADE para checar continuamente se a empresa está na direção e com os resultados esperados.

13

A abordagem de GOVERNANÇA
 Elementos essenciais 


Direcionadores e objetivos

Responsabilidades / estruturas de decisão

Gerenciamento de Riscos

Indicadores

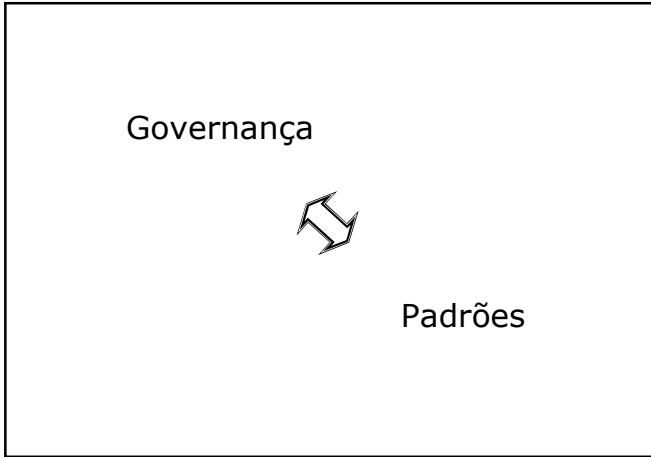
14

Quem deve usar GOVERNANÇA?
 Maiores movimentos em Governança. 

- Empresas Financeiras [30%]
- Governos (diretos e indiretos) [20%]
- Serviços [12%]
- Outros segmentos [< 5%]
 - Indústrias
 - Varejo

Fonte: ISACA

15



A Multiplicidade de Padrões
Dos objetivos de negócios à prática

CONTART

ISO9000	COSO	COBIT
ISO14000	Níveis da BOVESPA	ITIL
ISO27000	Basiléia II	CMMi
ISO20000	SOX (Sarbanes Oxley)	PMBok

17

- Porquê usar Padrões?**
Maiores movimentos em Governança.
- CONTART**
- Senso comum
 - Linguagem comum
 - Benchmarks
 - Atendimento às leis e normas setoriais ("compliance")
 - Incorporação de práticas de sucesso
- 18

Tipologia dos Padrões

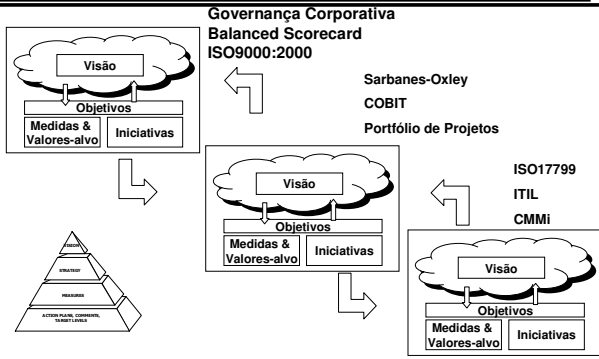
Maiores movimentos em Governança.



- Leis e Diretrizes Governamentais
 - SOX
- Normas Setoriais
 - BOVESPA, BC, ...
 - Basileia II
 - ISOs setoriais
- Alto Desempenho Gerencial/Melhores Práticas
 - BSC
 - COBIT, ITIL, CMMi,
 - ISOs

19

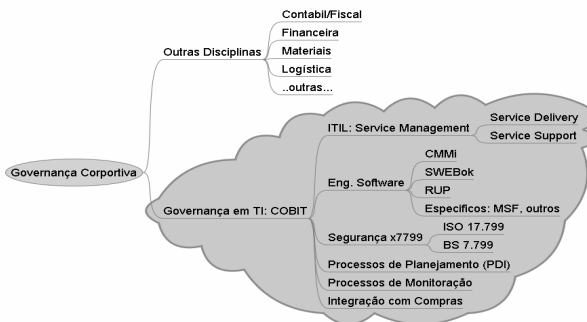
Estratégicos / Táticos / Operacionais
Dos objetivos de negócios à prática



20

GOVERNANÇA.


Dos objetivos de negócios à prática



21

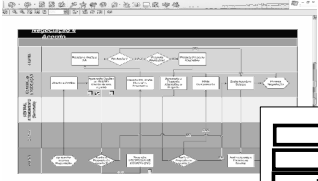
Padrões: Componentes Essenciais
 Dos objetivos de negócios à prática

Gerenciamento de Riscos
 Indicadores (KPIs, CSF)
 Atribuição de Responsabilidades
 Segurança e rastreabilidade
 Melhoria Contínua


 Intensa relação com Sistemas e T.I.
 Exigem abordagens processuais
 Necessitam educação e desenvolvimento de pessoal

22

O instrumento de ligação: PROCESSOS
 Trabalhando por processos



Objetivos e Métricas de Negócio

Capacidades Humanas e Organização

Fluxo das Atividades e Processamentos

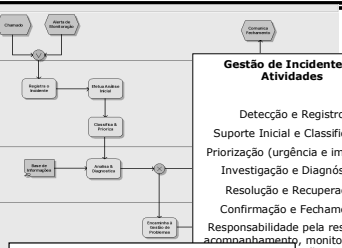
Dados (informações)

Recursos: Infra-Estrutura, Aplicativos

Quality Assurance

23

O instrumento de ligação: PROCESSOS
 Trabalhando por processos: modelando e gerenciando



Gestão de Incidentes :: Atividades

Deteção e Registro
 Suporte Inicial e Classificação
 Priorização (urgência e impacto)
 Investigação e Diagnóstico
 Resolução e Recuperação
 Confirmação e Fechamento
 Responsabilidade pela resolução e acompanhamento, monitorações, Gerenciamento

KPI :: Indicadores de Performance

Redução nos tempos de respostas aos incidentes

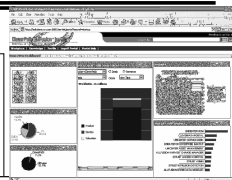
% de incidentes resolvidos pelos atendentes iniciais (primeiro nível)

% de redução nos incidentes encaminhados para responsáveis inadequados

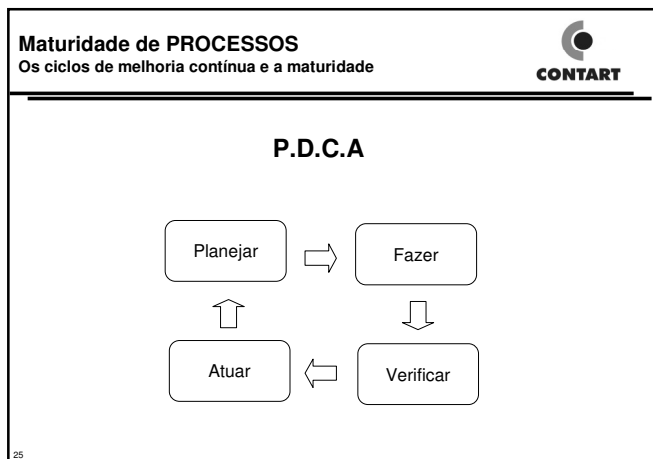
Indicadores de Call-Center (diversos)

Dados (problemas):

Registro do Problema (e seus atributos)
 Registro de Erros Conhecidos
 Relatórios estatísticos e gerenciais
 Apontam áreas frágeis em SI e TI
 Base de "workarounds"
 RFCs



24



25

Maturidade de PROCESSOS
Os ciclos de melhoria contínua e a maturidade

Nível	Característica	
5	Diferencial competitivo. O foco é o processo contínuo de aprimoramento. O impacto de novos processos, atividades e tecnologias podem ser previstos, avaliados e implementados quando necessários. Há total alinhamento e integração dos processos de TI com a dimensão de negócio. Proatividade.	OPTIMIZED
4	Métricas são adotadas para gerir a produtividade, avaliar os processos e os produtos. A entrega dos serviços são totalmente previsíveis e a qualidade é consistentemente elevada. Interfaces com outras áreas muito bem definidas. Forte alinhamento com demandas de negócios	MANAGED
3	Suporte organizacional integrado. Processo definido e publicado. Eficácia na alocação de recursos aos processos. Boa documentação. Treinamento são utilizados para garantir a adequação de equipes e rotinas.	DEFINED
2	Processos reconhecidos, mas com poucos recursos alocados. "Tracking" dos atendimentos, ações reativas. Atividades irregulares/não planejadas. É possível repetir práticas de sucesso. Ainda depende de iniciativa isoladas.	REPEATABLE
1	Caos, pânico periódico, esforços individuais e heróicos, ausência de processo e controles. Não é possível prever a repetição de êxitos e práticas de sucesso.	INITIAL

Definição e Adoção (seta apontando para nível 2)
Diferencial Competitivo – Forte Alinhamento (seta apontando para nível 5)


26

A relação com Sistemas e T.I.
Explorando as evoluções tecnológicas

- Ferramentas de Gerenciamento de Riscos
- Dashboards = Indicadores (KPIs, CSF)
- BPMS: Business Process Management Systems
- Gerenciamento Integrado de Segurança
- Gerenciamento Corporativo de Projetos (Mudanças)

27

A estrutura organizacional
 Surgem os "Escritórios de Governança"




O Escritório de Governança:

Responsável pela Formalização e Difusão da GC - Governança Corporativa.
 Facilitador na escolha, adoção e sinergia entre os diversos padrões.
 Suporta a introdução e adoção de práticas alinhadas com a GC.
 Integra as disciplinas-chaves (riscos, segurança, rastreabilidade, outras).
 Promove as capacitações necessárias.
 Monitora as responsabilidades dos demais setores.

Três grandes responsabilidades:
 Implantar
 Operar
 Aprimorar

Síntese
 Governança, Padrões e Tecnologia de Informação




Governança:

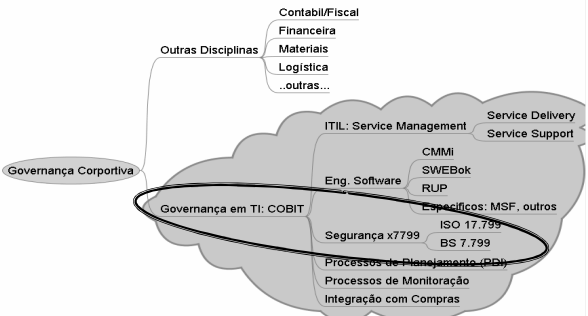
Padrões:

Tecnologia de Informação:

- Essencial e nuclear nas abordagens de Governança
- Essencial para a adoção dos padrões
- Habilita o trabalho por processos
- Fornece indicadores
- Habilita a gestão de segurança e rastreabilidades

GOVERNANÇA.
 Dos objetivos de negócios à prática





The diagram illustrates the scope of Corporate Governance, which includes various disciplines such as Accounting/Fiscal, Finance, Materials, Logistics, and others. It also shows the integration of IT Governance, which encompasses ITIL (Service Management, Service Delivery, Service Support), CMMI, SWEBok, RUP, and specific standards like ISO 17.799 and BS 7.799. Additionally, it lists processes such as Planning (PD), Monitoring, and Integration with Purchases.

GOVERNANÇA em TI: O COBIT
O modelo abrangente aceito pelo mercado

CONTART

GOVERNANÇA CORPORATIVA
direciona e define

GOVERNANÇA DE TI

Objetivos de Controle para Informação e Tecnologias
Relacionadas
Orientação ao **Negócio**
Gerenciamento de **Risco** da Informação e da TI
Retorno de Investimento
Controles "geralmente aplicáveis e aceitos"

MONITORAMENTO
M1 Monitorar os processos
M2 Avaliar a adequação dos controles internos
M3 Obter avaliação independente
M4 Disponibilizar-se para auditoria independente

PLANEJAMENTO E ORGANIZAÇÃO
PO1 Definir a estratégia de TI
PO2 Definir a arquitetura de TI
PO3 Definir a estrutura organizacional de TI
PO4 Definir a governança de TI
PO5 Definir a segurança da informação
PO6 Definir a continuidade de negócios
PO7 Definir a recuperação de desastres
PO8 Definir a gestão de mudanças
PO9 Definir a gestão de fornecedores
PO10 Definir a gestão de contratos
PO11 Definir a gestão de ativos de TI
PO12 Definir a gestão de riscos de TI
PO13 Definir a gestão de conformidade
PO14 Definir a gestão de incidentes
PO15 Definir a gestão de vulnerabilidades
PO16 Definir a gestão de patches
PO17 Definir a gestão de backups
PO18 Definir a gestão de logs

ENTREGA E SUPORTE
SI1 Definir a estratégia de TI
SI2 Definir a arquitetura de TI
SI3 Definir a estrutura organizacional de TI
SI4 Definir a governança de TI
SI5 Definir a segurança da informação
SI6 Definir a continuidade de negócios
SI7 Definir a recuperação de desastres
SI8 Definir a gestão de mudanças
SI9 Definir a gestão de fornecedores
SI10 Definir a gestão de contratos
SI11 Definir a gestão de ativos de TI
SI12 Definir a gestão de riscos de TI
SI13 Definir a gestão de conformidade
SI14 Definir a gestão de incidentes
SI15 Definir a gestão de vulnerabilidades
SI16 Definir a gestão de patches
SI17 Definir a gestão de backups
SI18 Definir a gestão de logs

AQUISIÇÃO E IMPLEMENTAÇÃO
AI1 Identificar soluções automatizadas
AI2 Adquirir e manter softwares aplicativos
AI3 Adquirir e manter a infraestrutura tecnológica
AI4 Desenvolver e manter procedimentos
AI5 Instalar e homologar os sistemas
AI6 Gerenciar as mudanças

Governança e Segurança de Informação
O padrão mais aceito pelo mercado: x7799 - Evolução

CONTART

1987 Criação do CCSC

1989 Users Code of Practice

1993 BS 1993, DISC PD0004

1995 BS 7799:1995

1999 AS/NZS 4444, BS 7799:1999

2000 ISO/IEC 17799:2000

2002 BS 7799-2:2002

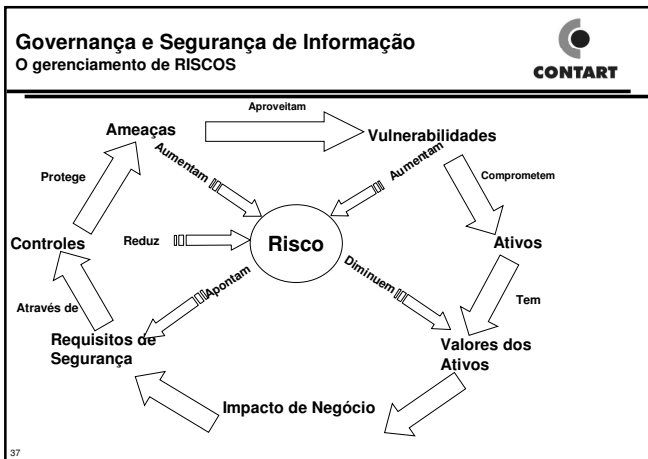
2005 ISO/IEC 17799:2005

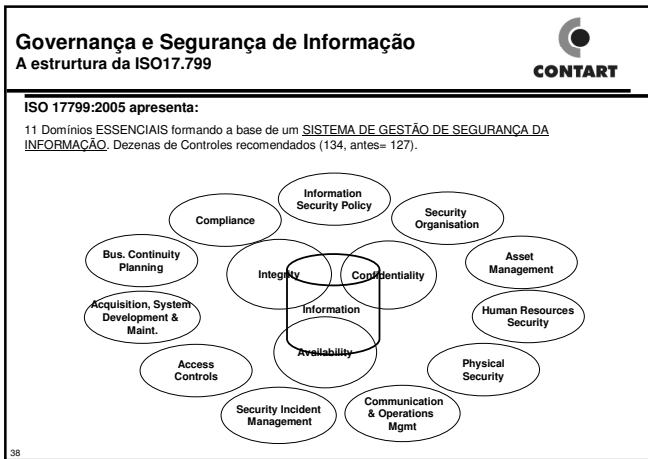
Gráfico de Evolução (2002-2005):
2002: 0
2003: ~250
2004: ~500
2005: ~1100

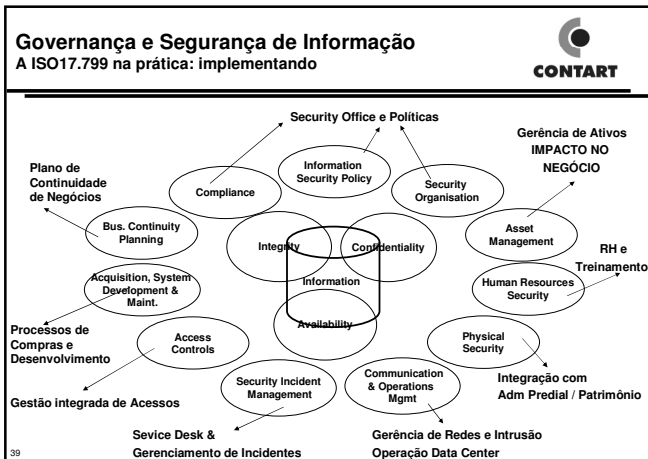
Governança e Segurança de Informação
x7799 será a Família ISO27000

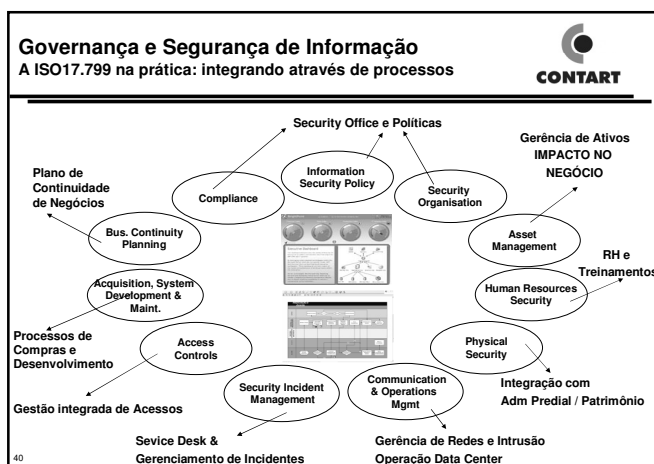
CONTART

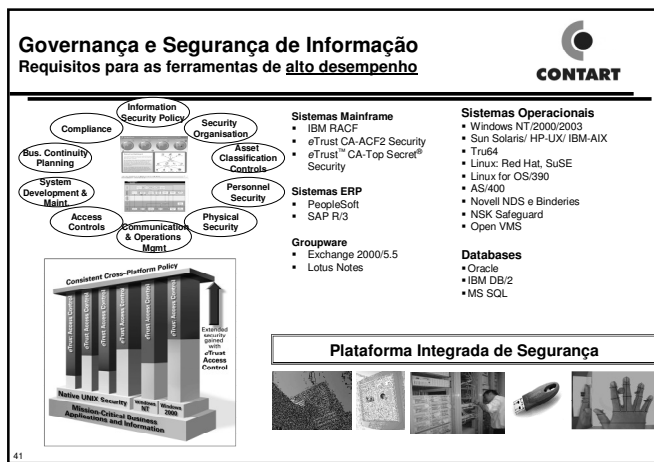
- ISO/IEC 27001 (BS7799-Part 2) - 'Information Security Management System'. (Once ISO/IEC 27001 is released, BS7799-2:2002 will be withdrawn)
- ISO/IEC 27002 (ISO/IEC 17799 & BS7799- Part 1) - The planned 'Code of Practice' replacement for ISO/IEC 17799:2005 scheduled for April 2007
- ISO/IEC 27003 (BS7799-3) 'Risk Assessment'. No announcement has yet been made regarding ISO/IEC 27003
- ISO/IEC 27004 (BS7799-4) 'Information Security Metrics and Measurement'. No launch date is available.












- ### Governança e Segurança de Informação
- Requisitos para as ferramentas de alto desempenho
- Permitir abordagem *por processos*
 - Intenso uso de *indicadores* e alertas
 - Integrar múltiplas tecnologias criando *visão unificada de segurança*
 - Aproveitar os *ativos existentes*
 - Integração com Service Desk e *Gerenciamento de Incidentes*
 - Facilitar o gerenciamento e atendimento de *serviços comuns de segurança* (redução de custos).
 - Suportar planos de *continuidade*
 - Suportar *bases de conhecimento* de segurança
 - Integração com *Gerenciamento de Ativos*
- A CA possui a plataforma mais robusta e abrangente para segurança de informação*

Síntese



- ❑ Ameaças e custos crescentes em segurança de informação
- ❑ Exigências maiores do acionistas e do mercado
- ❑ Governança: Normas ISO17799 é padrão de fato em Segurança
- ❑ Trabalhar com visão de RISCOS e CUSTOS - alinhamento ao negócio
- ❑ Trabalhar por processos, indicadores e maturidade
 - ❑ Seguir os processos padrões e buscar a maturidade
- ❑ Adotar ferramentas de alto desempenho e integração

43




Consulte nossa página
www.dromostg.com.br

OBRIGADO !

44

O desafio da segurança de Informação

Casos BRASILEIROS (clientes) recentes ...



Grande empresa de transporte e logística: roubo de dados comerciais na saída de profissional da área >> perda de clientes, chaves e contratos para a concorrência.

Grande empresa de processamento de meios de pagamento: Coordenador de área operacional com acesso e réplica completa da base de dados corporativa de clientes em seu micro pessoal.

Indústria multinacional do setor mineral: Conexão de equipamentos externos (notebooks) na rede permite acesso a aplicativos, alteração e cópia de informações através da intranet.

Maior universidade privada de importante estado brasileiro: Funcionário manipula dados de alunos alterando resultados de avaliações diretamente nas bases de dados.

Vários Clientes: Descontrole sobre acesso à diretórios, dados e sistemas. Inexistência de fluxos básicos de ativação e suspensão de acessos.

45
