FIAP

MBA+

# GESTÃO DE CIBERSEGURANÇA

FIAP

MBA+

# Data Loss Prevention e Classificação da Informação

**Profª Marcelo Barbosa Lima,**
**CISSP, ISAAP, CISM, MCSO, MBA.**
EMAIL mb_lima@uol.com.br

Abril de 2023

# PERDA DE DADOS

# Perda de Dados?

- **Vazamento de Dados**
- Problemas em unidades de armazenamento;
- Falhas no Backup;
- Deleção acidental;
- ...

# Na pauta das Organizações há muito tempo...


# Governança de Dados


*Em set/2020

**Fonte:** https://aws.amazon.com/pt/blogs/aws-brasil/ferramentas-de-governanca-de-dados-na-amazon-web-services/

# Quem deve se preocupar com vazamento de dados?

# Vazamento de Informação

## A quem interessa?
## Roubo de informações sobre campos de petróleo descobertos pela Petrobras pode ser espionagem

- Da pior forma possível, a Petrobras descobriu que a cobiça por informações sobre o campo petrolífero de Tupi, o maior do País, é mais forte que seu esquema de segurança. Na ação que é considerada a mais ousada de espionagem industrial no Brasil, criminosos roubaram um disco rígido e notebooks carregados de informações e avaliações técnicas sobre os megapoços em águas profundas recém-descobertos pela estatal. O crime foi constatado no dia 31 de janeiro, em Macaé (RJ), e tornado público na quinta-feira 14. "Houve um furto de equipamentos e materiais que continham informações importantes", admitiu, secamente, a Petrobras em nota. **Mais do que informações sobre os poços de petróleo, o ladrão ou ladrões teriam levado estudos feitos por especialistas sobre as condições geológicas daquela região.**
- Ou seja, serviço completo. **"A empresa levou décadas para levantar esses dados e gastou US$ 2 bilhões para isso", relata Fernando Siqueira, diretor da Associação de Engenheiros da Petrobras. "Esse material será útil para quem vier a atuar na exploração dos poços", diz.**
-

**•Fonte: ISTOÉ. Fevereiro de 2008**

# Vazamento de Informação

## Femsa aciona AmBev para tirar Puerto del Sol da rua

G1

/ ECONOMIA E NEGÓCIOS

30/11/2006 - 13h22m - Atualizado em 30/11/2006 - 13h25m Valor

**JUSTIÇA MANDA AMBEV TIRAR CERVEJA PUERTO DEL SOL DO MERCADO**

RSS Imprimir Enviar por e-mail Receber Newsletter

Tamanho da letra A- A+

tv globo
Jornal Nacional
Jornal da Globo
Jornal Hoje
Bom Dia Brasil
Fantástico
mais programas
globo news
Em Cima da Hora

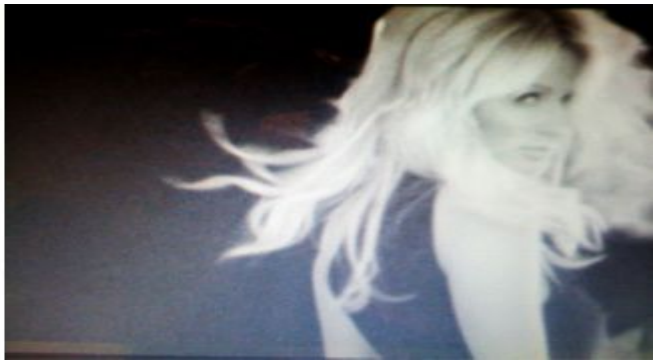
SÃO PAULO - A AmBev terá de tirar sua cerveja Puerto del Sol do mercado, além de toda a comunicação da marca, por decisão da Justiça de São Paulo que ontem julgou o mérito de liminar requerida pela Femsa em maio. Na ação, a cervejaria mexicana questionava a similaridade do produto da AmBev com o seu, a cerveja Sol.

A AmBev diz que não vai se manifestar porque a decisão ainda não foi publicada no " Diário Oficial " . Mas, segundo um executivo ligado à companhia, a empresa deve recorrer ao Superior Tribunal de Justiça (STJ), em Brasília para manter sua marca no mercado.

- (...) Oficialmente, nenhuma das duas cervejarias AmBev e Femsa assume o novo " round ". Nos bastidores, porém, travam uma disputa judicial que indica um confronto muito além das gôndolas. A Femsa Cerveja entrou na Justiça para impedir a venda e veiculação de publicidade da cerveja Puerto del Sol. A empresa mexicana, dona da marca Sol, acusa a AmBev de concorrência desleal e alega que o produto foi lançado para confundir o consumidor.
- (...) aposta da Femsa no mercado brasileiro e será o carro-chefe da companhia, que está investindo cerca de R$ 250 milhões numa campanha publicitária assinada por Eduardo Fischer. A marca foi " abrasileirada " , com nova fórmula e embalagens, para concorrer com as principais marcas do mercado. A AmBev nega que o lançamento de Puerto del Sol tenha sido um contra-ataque antecipado à chegada da Femsa no Brasil. Segundo a cervejaria, o produto estava previsto antes da chegada da Femsa ao Brasil. A Kaiser vende Sol no país desde 2001.

# Vazamento de Informação

**A Devassa parte pra cima**
**Com uma estratégia ousada, a cervejaria Schincariol lança um novo produto, surpreende a concorrência e tenta conquistar espaço em regiões onde sempre patinou**

- (...) Manter a estratégia em sigilo era fundamental. A AmBev, por exemplo, **tem profissionais dedicados a monitorar o mercado e descobrir possíveis novidades para que a empresa prepare contra-ataques.** A tática foi usada, por exemplo, antes do lançamento da Sol, da Femsa, em 2006 - a empresa começou a vender um produto batizado de Puerto del Sol, com a clara intenção de desgastar a cerveja rival que chegaria ao mercado meses depois. Para manter a Devassa Bem Loura em segredo, a Schincariol envolveu o menor número possível de pessoas em cada fase do projeto. Todos que tinham acesso às informações eram obrigados a assinar termos de confidencialidade com multas pesadas em caso de quebra de sigilo. Os 100 veículos que seriam utilizados para distribuição da nova cerveja foram guardados por 45 dias em um depósito em Paulínia, cidade do interior paulista localizada a cerca de 70 quilômetros da sede da cervejaria - só dentro do depósito eles receberam os adesivos Devassa. Os rótulos das garrafas foram impressos em gráficas no exterior para evitar o vazamento da informação. O contrato com Paris Hilton foi fechado em outubro e as gravações do comercial com ela ocorreram em Los Angeles. "No fim do ano, mais de 100 pessoas estavam envolvidas e todas guardaram segredo", diz Adriano.

**Fonte: Revista Exame, Março de 2010.**

# Vazamento de Informação


•A Ford pediu desculpas nesta sexta-feira por um **anúncio** envolvendo o ex-político e empresário italiano Silvio Berlusconi. A empresa reforçou também que o conteúdo, considerado ofensivo, não foi aprovado e **sua divulgação é fruto de um vazamento**.

•A agência JWT de Nova Déli, na Índia, criou uma campanha para promover o porta-malas do Ford Figo. Uma das peças exibe a figura de Berlusconi com, deduz-se, suas amantes amarradas.

•Enquanto ele faz o sinal de vitória com as mãos, as mulheres curvilíneas estão presas no porta-malas do carro. A imagem é arrematada pela frase "Deixe suas preocupações para trás".

•Ainda que o anúncio não tenha sido veiculado, até agora, em nenhuma **mídia** paga, sua performance na internet (e na imprensa italiana) não tem sido das melhores. As peças dividiram opiniões e foram classificadas por alguns como de mau-gosto e ofensivas.

•A reação negativa levou a Ford a manifestar-se hoje. A empresa pediu desculpas e afirmou que as peças jamais foram aprovadas, e vazaram para a web sem conhecimento oficial da companhia. “Lamentamos profundamente este incidente, que nunca deveria ter acontecido”, disse a empresa em email ao site Business Insider.

•Segundo o pronunciamento, “os cartazes são contrários aos padrões de profissionalismo e decência na Ford e nossos parceiros da agência”. A **marca** prometeu ainda rever os processos de aprovação e fiscalização de seus anúncios.

**Fonte: Revista Exame, Março de 2013**

# Vazamento de Informação

FIAP

**Wikileaks**

mundo

**WIKILEAKS** Segredos da Diplomacia

Saul Loeb - 17.abr.2011/France Presse

Porta-voz da secretária Hillary Clinton renuncia após críticas a caso WikiLeaks

colunistas

LUCIANA COELHO

**Criando um mártir**

CLÓVIS ROSSI

**Os painéis do site WikiLeaks**


## Embaixadora dos EUA sai do Equador após crise do WikiLeaks

O abandono ocorreu após o governo de Quito declarar que ela era "pessoa non grata"

- Equador acusa embaixada de espionagem
- Governo teme que rusgas afetem economia

MICROBLOG

**Juíza dos Estados Unidos mantém ordem para Twitter informar no caso Wikileaks**

PRESIDENTE

**Barack Obama defende tratamento dado a suspeito do WikiLeaks na prisão**

## EUA derrubam site que vaza documento secreto

Alerta da Interpol coloca fundador do WikiLeaks na lista dos mais procurados

Criticado por governantes e países afligidos pela divulgação de documentos secretos de sua diplomacia, o governo dos EUA conseguiu tirar do ar por pelo menos cinco horas o site WikiLeaks, autor do vazamento.

Por pressão feita pelo Departamento de Segurança Doméstica dos EUA e pela Comissão de Segurança Nacional do Senado americano, a Amazon, que fornecia servidores ao WikiLeaks, retirou o serviço do ar.

No final da tarde, o site voltou a ser acessado por intermédio de um servidor europeu. A Amazon Web Services — parte da Amazon.com, popular site de venda de livros e outros produtos — não quis comentar.

A pedido de corte sueca, a Interpol (polícia internacional) colocou Julian Assange, fundador do WikiLeaks, na lista dos mais procurados. Ele é acusado de crimes sexuais e coerção ilegal. Assange nega. Pág. A12 e A15

Siga a Folha de S.Paulo no Twitter Seguir

**as últimas que você não leu**

1. Ataques na Nigéria deixam 25 mortos
2. Cidades pelo mundo apagam as luzes para Hora do Planeta
3. Grupo rebelde curdo formaliza cessar-fogo em conflito na Turquia
4. Oposição venezuelana denuncia abuso de poder em campanha governista
5. Livre após 23 anos na prisão injustamente, homem sofre ataque card

# Vazamento de Informação

FIAP

**Vatileaks**

G1 | MUNDO

NET

buscar

Editorias | Economia | Sua região | Telejornais | Serviços | VC no G1 | Princípios editoriais | Novo Papa | IR 2013 | Lollapalooza

26/05/2012 10h52 - Atualizado em 26/05/2012 10h59

## Vaticano confirma que preso em caso 'Vatileaks' é o mordomo de Bento XVI

Paolo Gabriele teria sido encontrado com documentos secretos.
Polícia investiga vazamento de notícias reservadas.

Do G1, com agências internacionais

22 comentários | Tweetar 86 | Recomendar 169

Magistrados do **Vaticano** oficializaram neste sábado (26) a acusação contra o mordomo do Papa em respeito à posse de documentos secretos após vazamentos que geraram polêmica na Santa Sé. A mídia local já havia antecipado que a prisão ocorrida esta semana no caso fora justamente do mordomo, Paolo

PUBLICIDADE


**Seus amigos leram...**

Juliana leu há 2 dias
Jovem filmada sendo agredida é encontrada morta, em Anápolis,...

Juliana leu há 3 dias
Pai filmado agredindo alunas diz que filha era ameaçada na...

# Vazamento de Informação

**Orgão da Administração Pública no Brasil**

Início » Antivírus e Segurança » Exclusivo: vazamento que expôs 220 milhões de brasileiros é pior do que se pensava

## Exclusivo: vazamento que expôs 220 milhões de brasileiros é pior do que se pensava

Vazamento inclui CPF, foto de rosto, endereço, telefone, e-mail, score de crédito, salário e mais; Serasa nega ser fonte dos dados

Por Felipe Ventura
22/01/2021 às 14:10

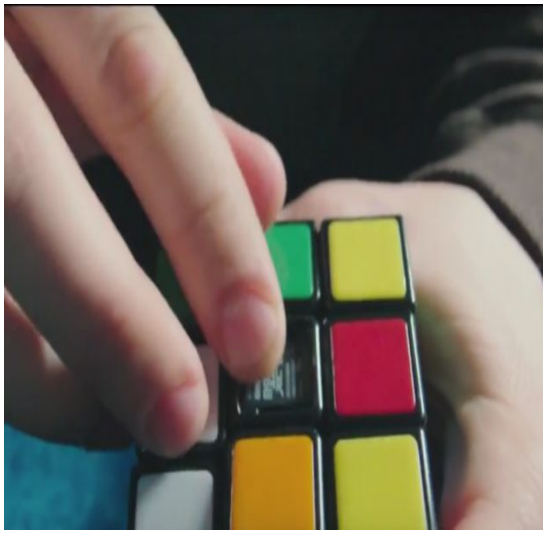
NEWS

Esta semana, surgiu a notícia de um **vazamento** enorme que expôs o CPF de mais de 220 milhões de brasileiros. O **Tecnoblog** descobriu que o caso é mais grave: esse conjunto de dados pessoais, oferecido de graça em um fórum de internet, está associado a uma base ainda maior que inclui foto de rosto, endereço, telefone, e-mail, score de crédito, salário, renda e muito mais. O arquivo parece estar associado à Serasa Experian, mas a empresa nega ser a fonte.

# Vazamento de Informação

FIAP

**NSA**

# Vazamento de Informação

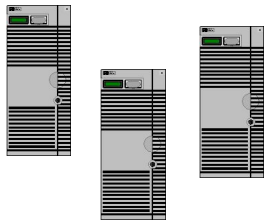
FIAP

**CIA**



# UMA TECNOLOGIA PARA PREVENÇÃO

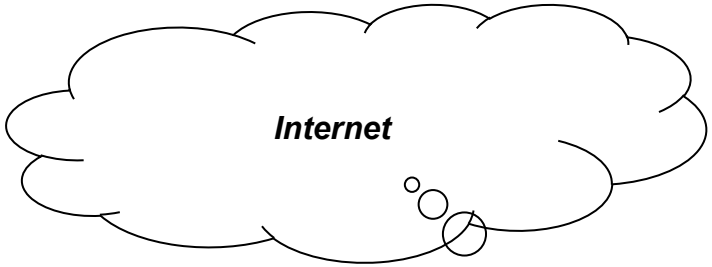
# Onde a informação precisa ser Protegida por uma ferramenta de DLP?



***Servidores / Pastas de Rede***

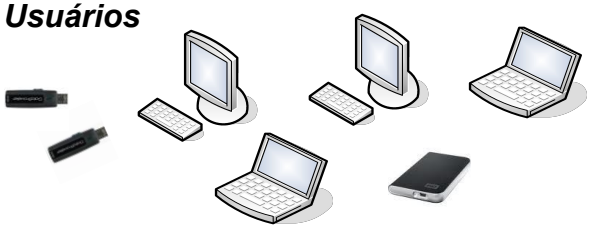
Data at Rest – Verificação de repositórios estacionários (ex.: arquivos da rede)

Data at the Endpoint – Verificação de informações armazenadas em notebooks e dispositivos portáteis (USB, CD/DVDs, etc.)



***Internet***

***Estações de Trabalho / Usuários***



Data in Motion – Verificação de informação transmitida para fora da rede da empresa (e-mail, web, etc.)

# UMA TECNOLOGIA RESOLVE TUDO?

# Atividade

Em uma investigação sobre um vazamento recente, o time de segurança da informação verificou que um usuário fez diversos acessos a um banco de dados e provavelmente está vendendo informações confidenciais para concorrentes. A solução de DLP não gerou qualquer alerta. Ou seja, não conseguiram confirmação do roubo de informações por e-mail, mídias de armazenamento removíveis, upload na nuvem (dropbox, Gdrive e similares), softwares de comunicação populares, etc. O único fato estranho é que na máquina encontraram apenas muitos arquivos de áudio/músicas. Foram olhar os binários instalados e encontraram alguns fora do padrão da organização:

- Winrar
- Spotify
- Popcorn
- Stremio
- DeepSound
- Zoom
- Dropbox
- Steam

Uma amostra pequena dos arquivos de áudio pode ser encontrada aqui. O que você pode concluir deste cenário? Quais seriam suas recomendações para evitar este tipo de vazamento?

# Tecnologias de DLP não são Suficientes para Prevenir Perda de Dados

- Ferramentas de DLP precisam ser parametrizadas, tal que sejam capazes de identificar dados confidenciais de uma organização
- Após parametrização para a identificação de dados confidenciais, a ferramenta de DLP deve receber políticas para prevenção de vazamentos.
- Um projeto de DLP, portanto, exige o envolvimento de todas as áreas de negócios.
- Soluções de DLP não conseguem parar vazamentos intencionais

# Tecnologias de Segurança não são Suficientes para Prevenir Perda de Dados

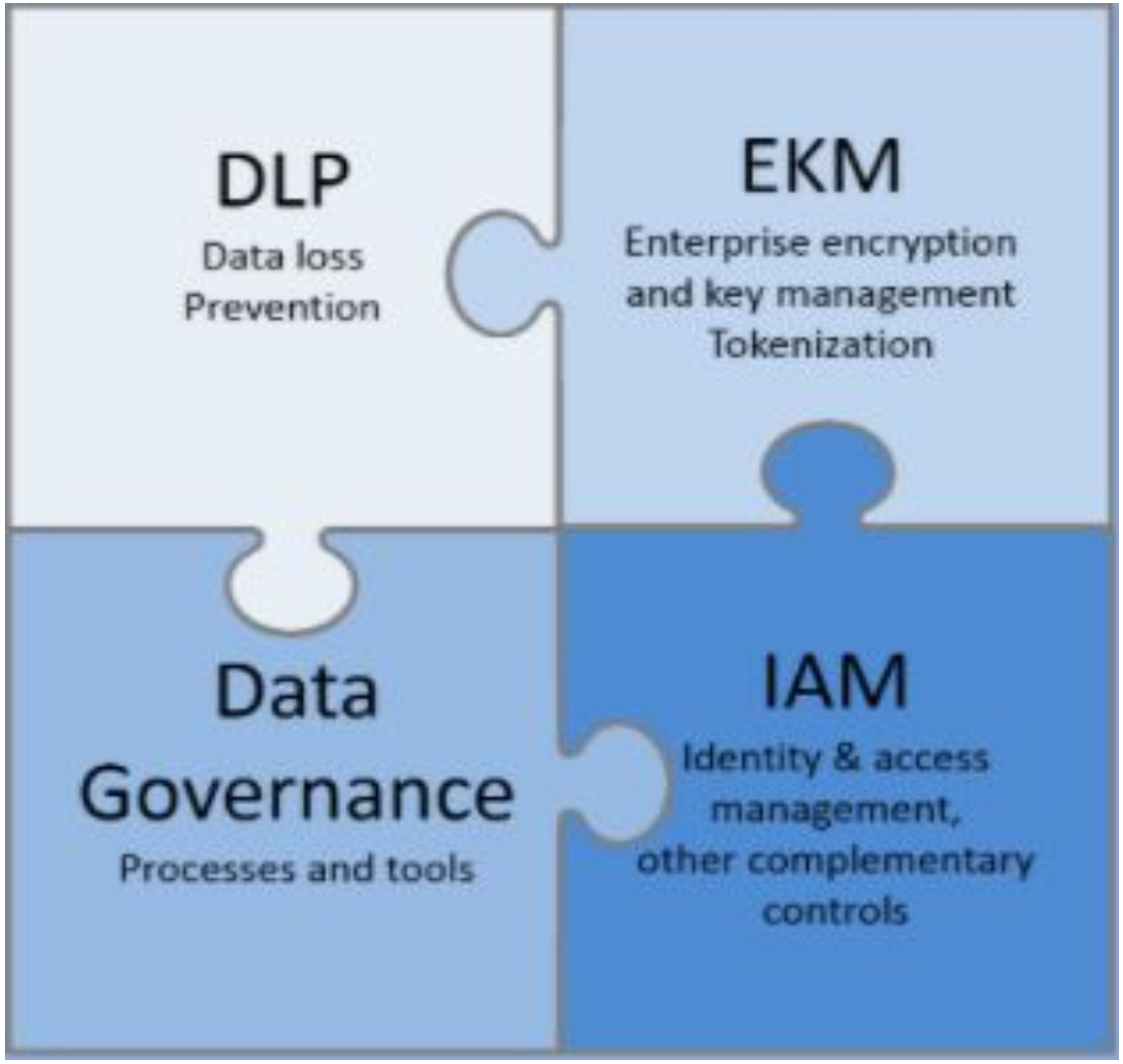
FIAP

"Se você acredita que a tecnologia pode resolver seus problemas de segurança, então você não conhece os problemas e nem a tecnologia."


Bruce Schneier

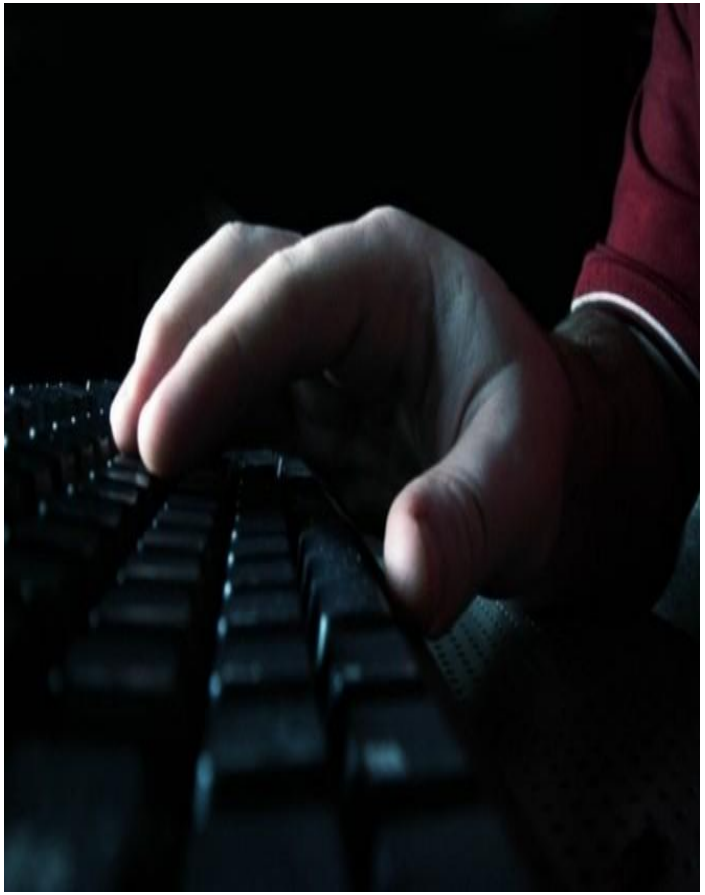
Schneier, Bruce - Segurança.com (secrets and lies), Ed. Campus, 2001, Rio de Janeiro, pg. 12

# Data Loss Prevention É UM PROGRAMA



# VAZAMENTO DE INFORMAÇÕES

# Conceito



- Qualquer divulgação não autorizada de informação que resulte no comprometimento da confidencialidade de ativos internos, proprietários ou sensíveis.

- Acontece quando a informação é revelada intencionalmente ou acidentalmente para pessoas não autorizadas. Esta informação pode ter natureza confidencial, tal como números de cartões de crédito, senhas e credenciais, cadastros de recursos humanos, dados financeiros ou quaisquer outras informações, que possam ser usadas por agentes maliciosos para explorar sistemas.

# Grandes Desafios para a Prevenção de Perda de Dados

# Colocando a Lupa nos Vazamentos, por que eles acontecem tão facilmente?

- Grande Volume de Dados
- Mídias de Armazenamento
- Shadow IT
- Informações espalhadas na Cloud
- Falta de conscientização dos Usuários e Engenharia Social
- Falhas na classificação da Informação
- Programas de Segurança da Informação pobres.
- ...

# Controles para prevenção de perda de dados

# Controles para Mitigar Riscos de Perda de Dados

- Classificação da Informação.
- Definição de políticas, processos e procedimentos adequados.
- Conscientização dos Usuários.
- Adoção de estratégias e soluções de backup.
- Mecanismos de controle de Acesso baseado no need-to-know dos usuários.
- Implantação de controles de acesso físico apropriados.
- Destruição segura da informação quando a mesma deixar de ser útil para os negócios ou por requisitos legais.
- Implantação de procedimentos e tecnologias de segurança física.
- Implementação de soluções tecnológicas para a prevenção à perda de dados.

# Como Informações estão vazando das Organizações?

# Impactos

## Quanto Custa o Vazamento das Informações?

- Vantagem Competitiva;
- Propriedade Intelectual;
- Investimentos com Pesquisa e Desenvolvimento de Novos Produtos;
- Campanhas de Marketing;
- Informações de Clientes (CRM);
- Planejamento Estratégico;
- Imagem da Organização;
- Multas (Legislação e Normas da Indústria);
- ...

# Vazamentos Acidentais

## Como ocorrem os Vazamentos Acidentais?

- Comentários e mensagens de erros em scripts, programas e similares;
- Metadados “escondidos” em arquivos;
- Informações disponíveis na rede (registro.br, informações indexadas por ferramentas de busca, etc.);
- Perda de mídias removíveis;
- Conversas em locais públicos;
- Posts em Mídias Sociais;
- Envio de informações confidenciais por e-mail;
- Material esquecido em Impressoras;
- Material deixado em cima de mesas e em salas de reunião;
- Falta de cuidado no descarte de informações;
- Envio de informações para contas pessoais;
- ...

# Vazamentos Intencionais

FIAP

**Como ocorrem os Vazamentos Intencionais?**

- Roubo de informações por agentes maliciosos internos;
- Furto de dispositivos móveis e/ou mídias de armazenamento;
- Cópia ou filmagem;
- Hacking;
- Acesso autorizado e cópia em mídias removíveis;
- Engenharia Social;
- Dumpster Diving/Trashing;
- ...

# Exemplos

- **Comentários do Desenvolvedor “Esquecidos” em Páginas de Resposta:**

- <TABLE border="0" cellPadding="0" cellSpacing="0" height="59“ width="591">
- <TBODY>
- <TR>
- <!--If the image files fail to load, check/restart **192.168.0.110** -->
- <TD bgColor="#ffffff" colSpan="5" height="17" width="587"> </TD>
- </TR>

# Exemplos

- **Mensagens de Erros Reveladoras**

An Error Has Occurred.
Error Message:
System.Data.OleDb.OleDbException: Syntax error (missing operator) in query expression **'username = '" and password = 'g**'. at System.Data.OleDb.OleDbCommand.ExecuteCommandTextErrorHandling ( Int32 hr) at System.Data.OleDb.OleDbCommand.ExecuteCommandTextForSingleResult ( tagDBPARAMS dbParams, Object& executeResult) at

# Exemplos: Metadados

# Exemplos: Metadados

## EXIF

| | |
|---|---|
| ImageDescription | |
| Make | NIKON |
| Model | COOLPIX P6000 |
| Orientation | Horizontal (normal) |
| XResolution | 300 |
| YResolution | 300 |
| ResolutionUnit | inches |
| Software | Nikon Transfer 1.1 W |
| ModifyDate | 2008:11:01 21:15:07 |
| YCbCrPositioning | Centered |
| ExposureTime | 1/75 |
| FNumber | 5.9 |
| ExposureProgram | Program AE |
| ISO | 64 |
| ExifVersion | 0220 |
| DateTimeOriginal | 2008:10:22 16:28:39 |
| CreateDate | 2008:10:22 16:28:39 |
| ComponentsConfiguration | Y, Cb, Cr, - |
| ExposureCompensation | 0 |
| MaxApertureValue | 2.7 |
| MeteringMode | Multi-segment |
| LightSource | Unknown |
| Flash | Off, Did not fire |
| FocalLength | 24.0 mm |
| UserComment | |
| FlashpixVersion | 0100 |
| ColorSpace | sRGB |
| ExifImageWidth | 640 |
| ExifImageHeight | 480 |
| InteropIndex | R98 - DCF basic file (sRGB) |
| InteropVersion | 0100 |
| FileSource | Digital Camera |
| SceneType | Directly photographed |
| CustomRendered | Normal |
| ExposureMode | Auto |
| WhiteBalance | Auto |
| DigitalZoomRatio | 0 |
| FocalLengthIn35mmFormat | 112 mm |
| SceneCaptureType | Standard |
| GainControl | None |
| Contrast | Normal |
| Saturation | Normal |
| Sharpness | Normal |
| SubjectDistanceRange | Unknown |
| GPSLatitudeRef | North |
| GPSLatitude | 43.467448 |
| GPSLongitudeRef | East |
| GPSLongitude | 11.885127 |
| GPSAltitudeRef | Above Sea Level |
| GPSTimeStamp | 14:27:07.24 |
| GPSSatellites | 06 |
| GPSImgDirectionRef | Unknown () |
| GPSMapDatum | WGS-84 |
| GPSDateStamp | 2008:10:23 |
| Compression | JPEG (old-style) |
| ThumbnailOffset | 4560 |

# Exemplos: Perda de Mídias de Armazenamento

**Pendrive com movimentações de tropas britânicas é encontrado em chão de boate**


•**Fonte**: http://www.gizmodo.com.br/tags/armazenagem/page/6/, Setembro de 2008.

# Exemplos: Informações espalhadas na Rede

## Google dorks

✓**Procurando planilhas contendo senhas**

"login: *" "password:*" filetype:xls

✓**Procurando servidores negligenciados**

intitle:"test page for Apache"

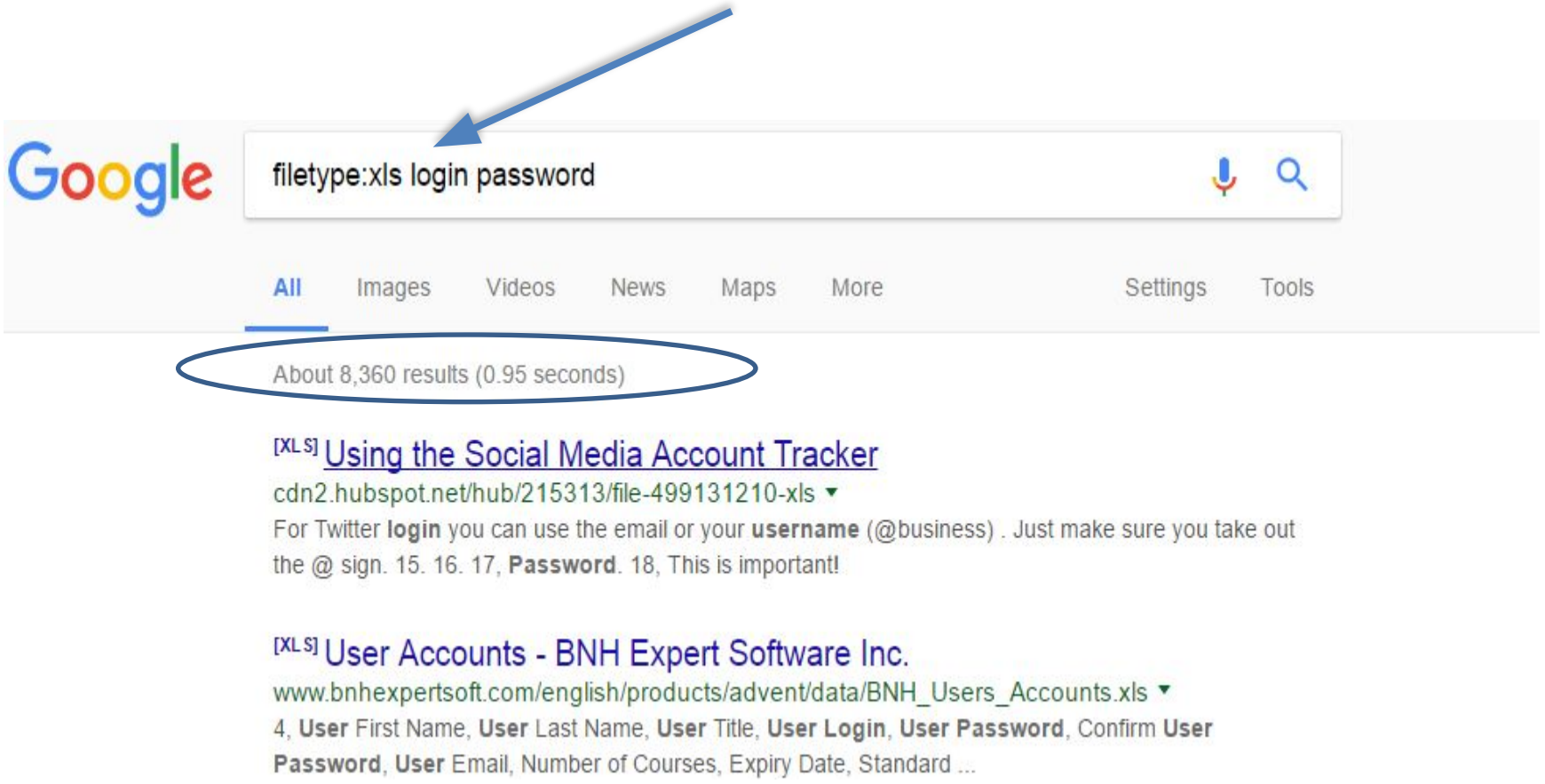
intitle:"Página teste para a instalação do Apache"

✓**Listagem de diretórios**

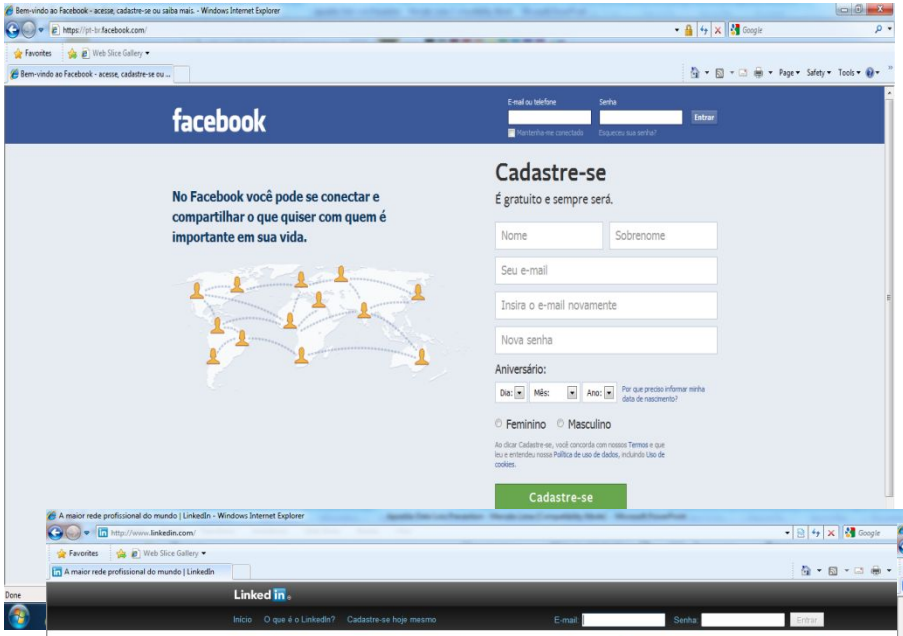
intitle:"index of" .htpasswd

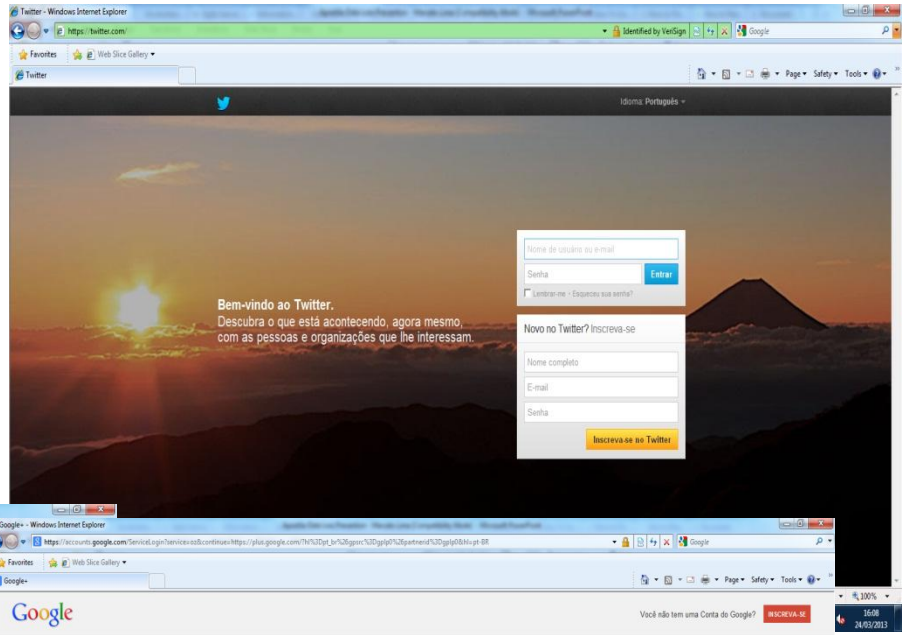
intitle:"index of" /admin

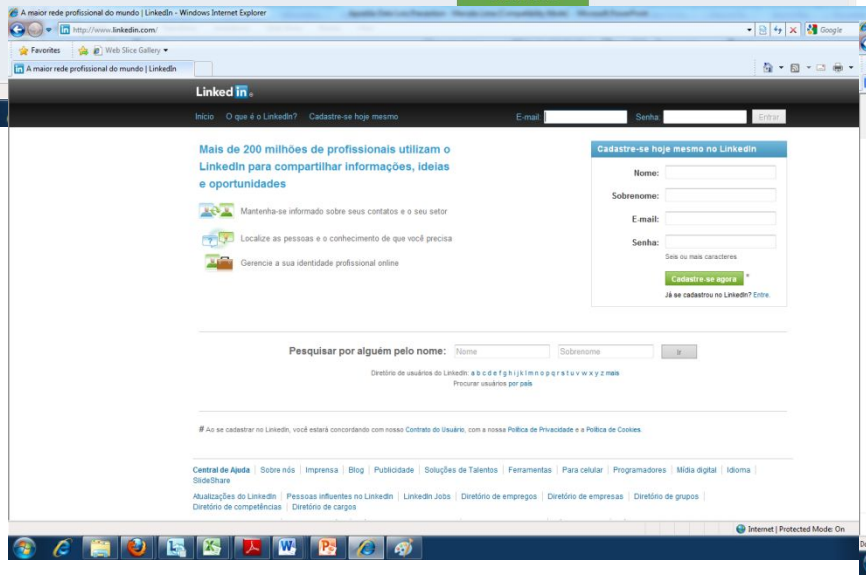
# Exemplos: Informações espalhadas na Rede

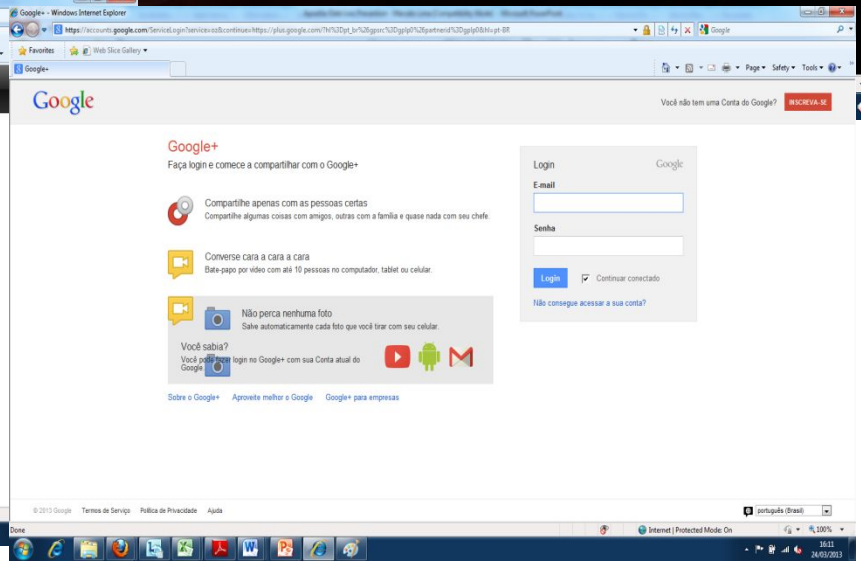


# Exemplos: Redes Sociais

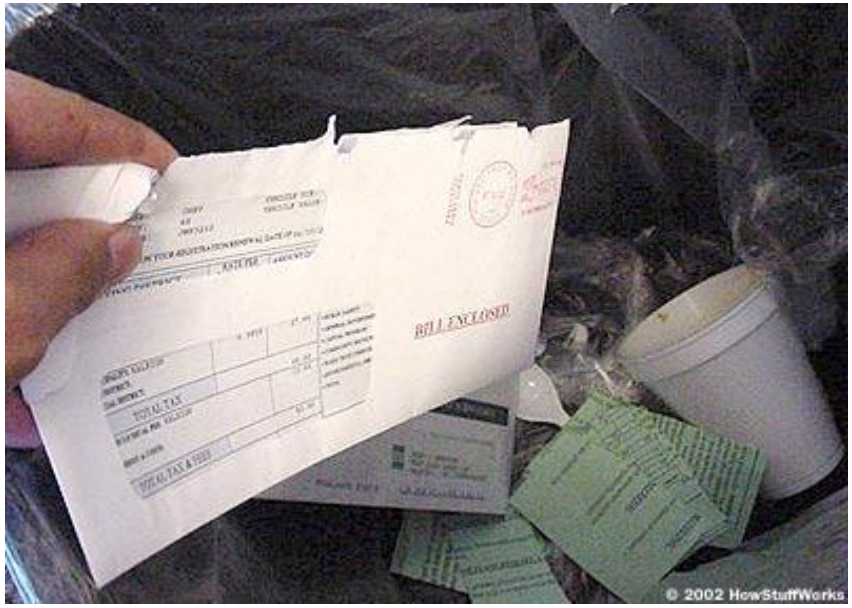


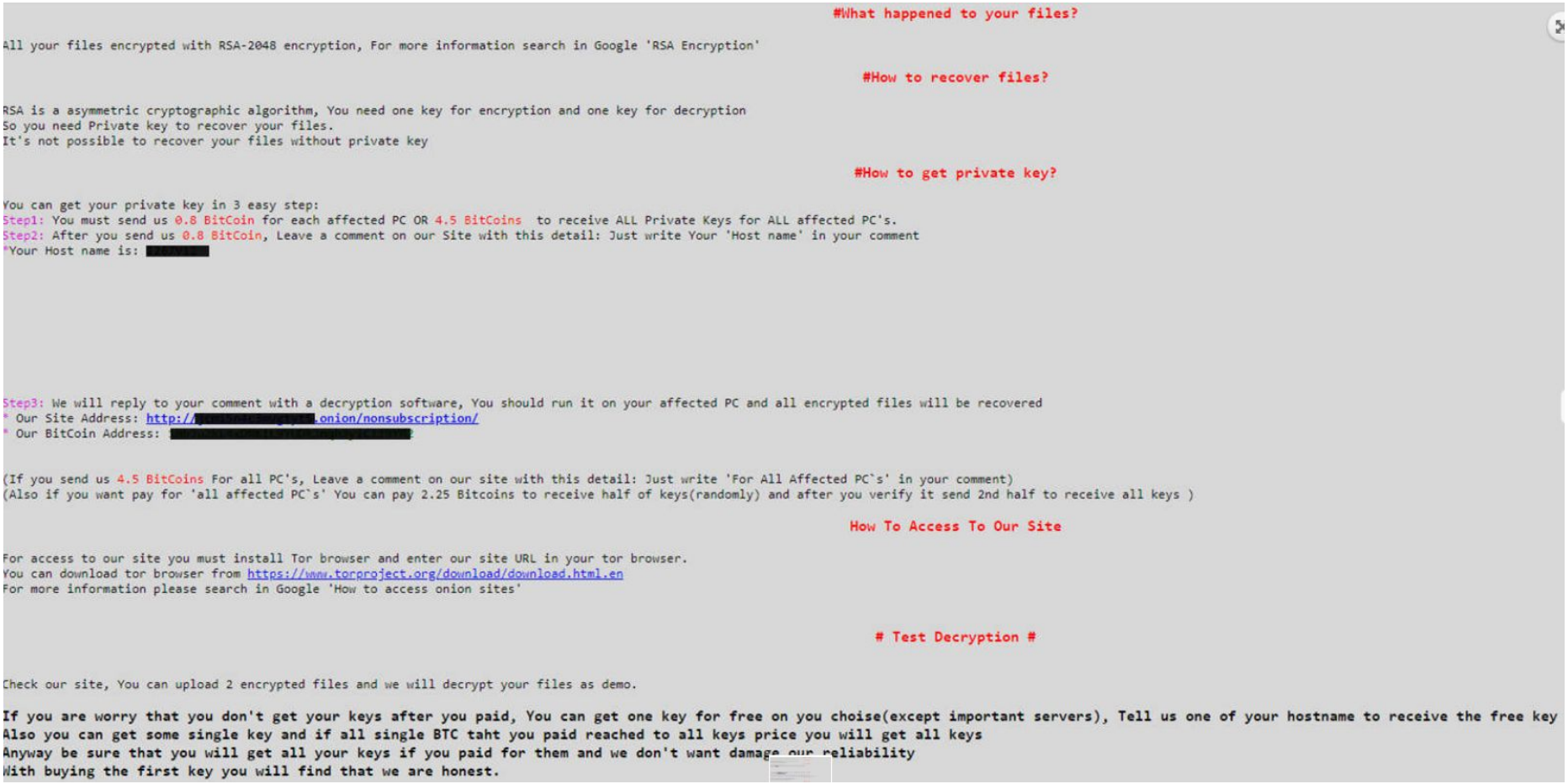



# Exemplos: Dumpster Diving ou Trashing




# Exemplos: Ransomware



#What happened to your files?

All your files encrypted with RSA-2048 encryption, For more information search in Google 'RSA Encryption'

#How to recover files?

RSA is a asymmetric cryptographic algorithm, You need one key for encryption and one key for decryption
So you need Private key to recover your files.
It's not possible to recover your files without private key

#How to get private key?

You can get your private key in 3 easy step:
Step1: You must send us 0.8 BitCoin for each affected PC OR 4.5 BitCoins to receive ALL Private Keys for ALL affected PC's.
Step2: After you send us 0.8 BitCoin, Leave a comment on our Site with this detail: Just write Your 'Host name' in your comment
*Your Host name is: [redacted]

Step3: We will reply to your comment with a decryption software, You should run it on your affected PC and all encrypted files will be recovered
* Our Site Address: http://[redacted].onion/nonsubscription/
* Our BitCoin Address: [redacted]

(If you send us 4.5 BitCoins For all PC's, Leave a comment on our site with this detail: Just write 'For All Affected PC`s' in your comment)
(Also if you want pay for 'all affected PC`s' You can pay 2.25 Bitcoins to receive half of keys(randomly) and after you verify it send 2nd half to receive all keys )

How To Access To Our Site

For access to our site you must install Tor browser and enter our site URL in your tor browser.
You can download tor browser from https://www.torproject.org/download/download.html.en
For more information please search in Google 'How to access onion sites'

# Test Decryption #

Check our site, You can upload 2 encrypted files and we will decrypt your files as demo.

**If you are worry that you don't get your keys after you paid, You can get one key for free on you choise(except important servers), Tell us one of your hostname to receive the free key**
**Also you can get some single key and if all single BTC taht you paid reached to all keys price you will get all keys**
**Anyway be sure that you will get all your keys if you paid for them and we don't want damage our reliability**
**With buying the first key you will find that we are honest.**

# CLASSIFICAÇÃO DA INFORMAÇÃO

# Objetivos

- ✓ Classificação da Informação é fundamental para o sucesso de qualquer programa de segurança da informação.
- ✓ Possibilita definir quais ativos de informação são importantes/críticos para o negócio.
- ✓ Permite a definição dos níveis de proteção e os controles a serem implementados ao longo do ciclo de vida da informação.
- ✓ Permite que a organização crie programas de segurança alinhados aos objetivos do negócio.
- ✓ Ajuda a empresa atingir objetivos de conformidade com leis, padrões e boas práticas da indústria (GDPR, PCI DSS, HIPPA, SOX, etc).
- ✓ Pode aumentar o nível geral de conscientização e engajamento em segurança da Informação.

# Ciclo de Vida da Informação

FIAP

# Processo de Classificação da Informação

# Inventário

- ✓ O propósito em se desenvolver um inventário de ativos é para que você saiba quais informações classificadas você tem em sua posse, e quem é responsável por elas (i.e., que é o proprietário).

- ✓ Informação pode estar em diferentes formatos e tipos de mídia, como por exemplo:

  - documentos eletrônicos
  - sistemas de informação / bases de dados
  - documentos em papel
  - mídias de armazenamento (ex.: discos, cartões de memória, etc.)
  - informação transmitida verbalmente
  - E-mail

- ✓ Possibilita identificar quando as informações podem e devem ser descartadas.

# Classificação da Informação

FIAP

- ✓ Em geral, o proprietário do ativo é o responsável por classificar a informação, com base nos resultados da análise/avaliação de riscos

- ✓ Quanto maior e mais complexa sua organização, mais níveis de confidencialidade você terá – por exemplo, para organizações de médio porte você pode utilizar este tipo de 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)

# Classificação da Informação

FIAP

- ✓ Uma organização pode ter mais de um esquema de classificação diferente implantado.

- ✓ Por exemplo, a OTAN requer a seguinte classificação com quatro níveis de confidencialidade e dois níveis públicos:

  - Cósmico Altamente secreto (Cosmic Top Secret)
  - OTAN Secreto (NATO Secret)
  - OTAN Confidencial (NATO Confidential)
  - OTAN Restrito (NATO Restricted)
  - OTAN Não Classificado (direito autoral) (NATO Unclassified (copyright))
  - INFORMAÇÃO NÃO SENSÍVEL LIBERÁVEL PARA O PÚBLICO (NON SENSITIVE INFORMATION RELEASABLE TO THE PUBLIC)

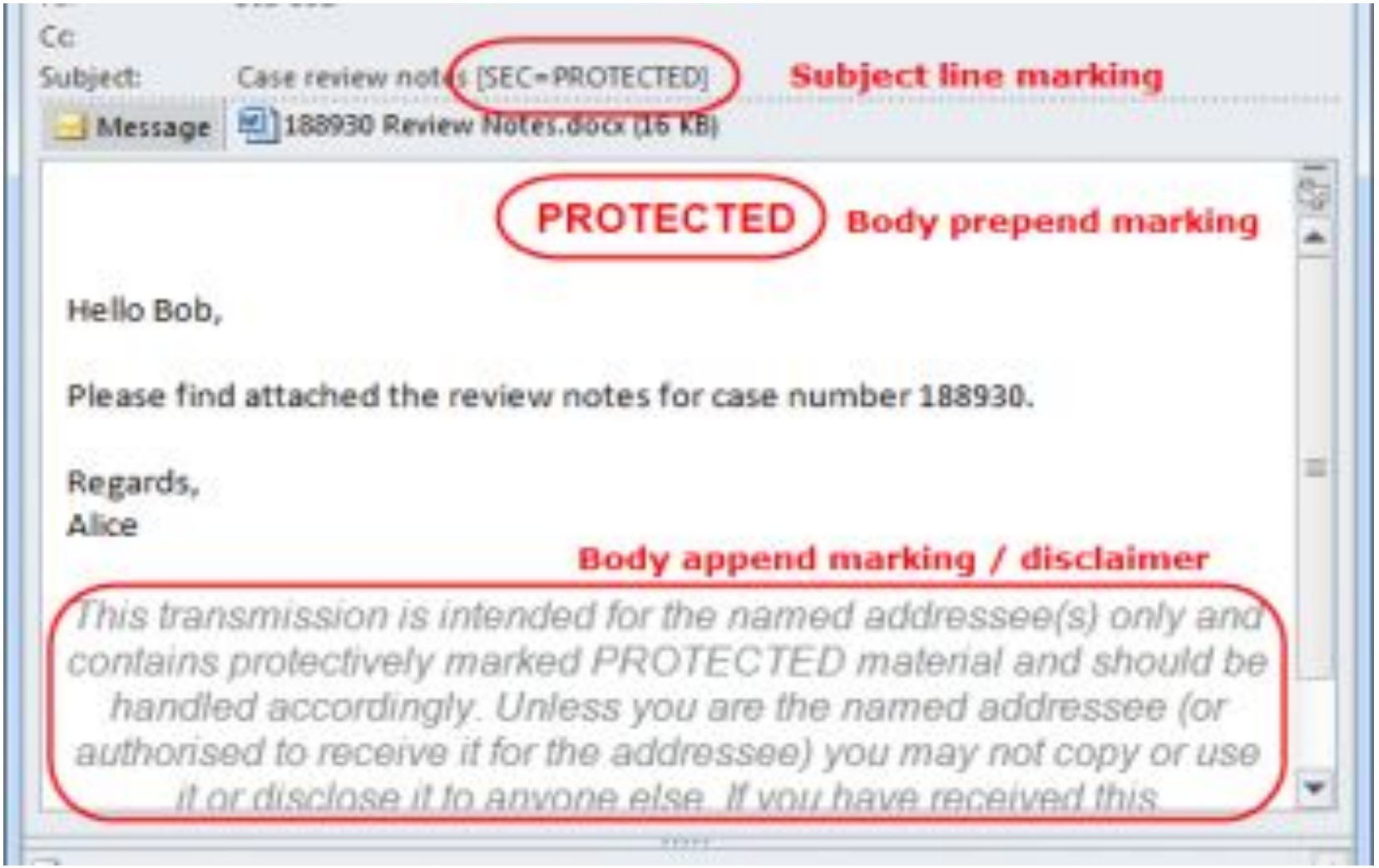
# Rotulagem da Informação

- ✓ Uma vez que você tenha classificado a informação, você precisará rotulá-la apropriadamente – você deveria desenvolver orientações para cada tipo de ativo de informação sobre como ele precisa ser rotulado.

- ✓ Por exemplo, você poderia definir as regras para documentos em papel de tal forma que o nível de confidencialidade seja indicado no canto superior direito de cada página do documento, e que a classificação também seja indicada na capa ou no envelope que transporta tal documento, assim como na pasta onde o documento é armazenado.

- ✓ A rotulagem da informação geralmente é responsabilidade do proprietário da informação.

# Rotulagem da Informação

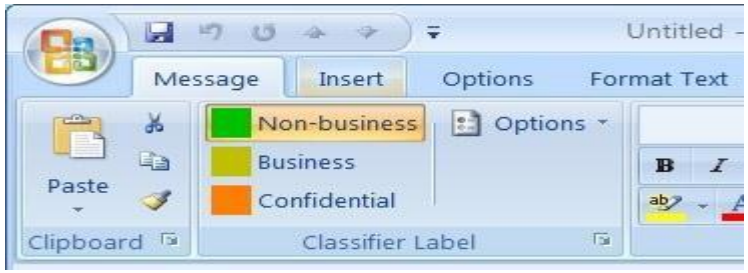


# Política de Uso da Informação

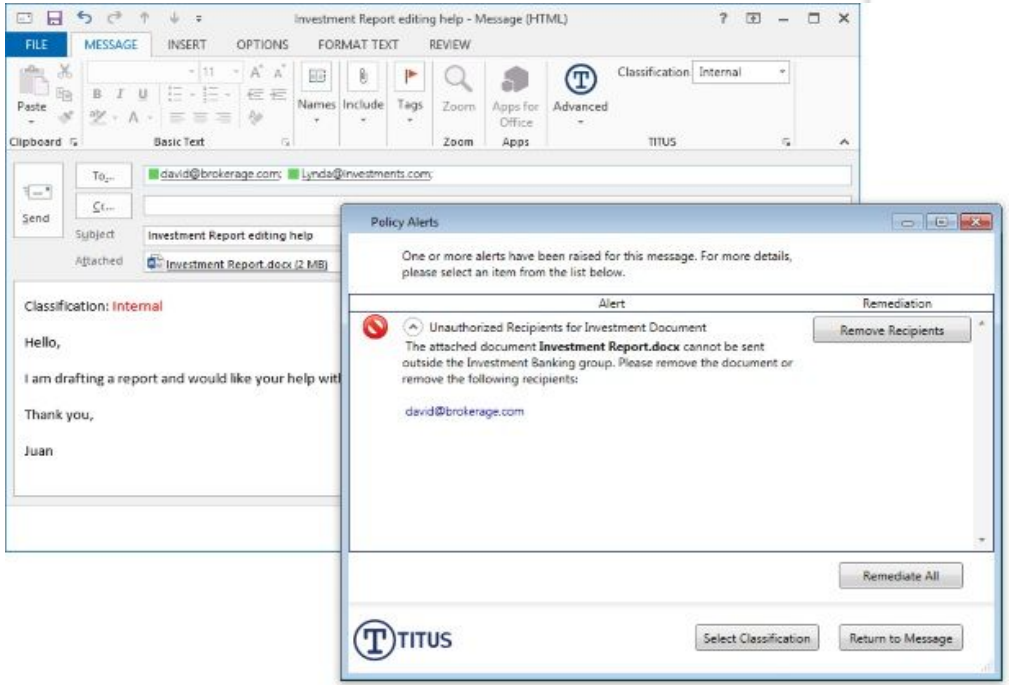
- ✓ A classificação da informação é parte fundamental para a definição de políticas e controles/salvaguardas para a proteção da informação.

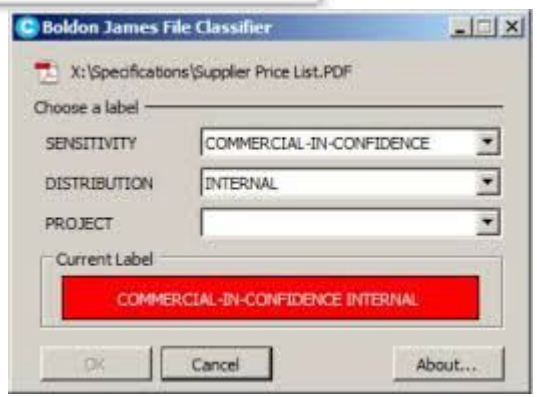
# Classificação da Informação

**Algumas ferramentas facilitam o trabalho de classificação da informação. Exemplos: Titus e Boldon James.**







# Atividade

# Atividade

Uma agência de viagens XPTO trabalha com as seguintes informações:

- Dados cadastrais dos clientes em bases de dados;
- Dados cadastrais de parceiros (companhias aéreas, hotéis, etc.) em bases de dados;
- Dados do portador de cartão de pagamento em cópias digitalizadas e impressas dos cartões do cliente;
- Histórico de viagens de clientes em bases de dados;
- Informações sobre pacotes turísticos divulgadas pela Web;
- Informações de Recursos Humanos em base de dados e impressas;
- Mensagens de correio eletrônico.

1. Quais níveis de classificação você criaria para esta agência? Explique o que significa cada um destes níveis propostos.
2. Para cada tipo de informação acima e usando os níveis de classificação propostos por você, como você classificaria tais informações?
3. Do ponto de vista dos riscos de vazamento, quais níveis precisam ser protegidos?
4. Qual a importância desta classificação para uma estratégia de DLP?
5. Dê uma sugestão de política de manuseio das informações.

# TUDO PRONTO PARA A IMPLEMENTAÇÃO DE UM PROCESSO DE DLP?

# Cenário 1

Você é o consultor responsável pela implantação de um processo e uma tecnologia de DLP. Você fez um rápido assessment na empresa cliente e percebeu:

1. **Baixo nível de maturidade em segurança.**
2. **Uma política de segurança foi escrita, mas não implementada totalmente.**
3. **Algumas informações são altamente confidenciais e manipuladas sem grandes cuidados. Pior: parte significante desta informação sequer é classificada.**
4. **Ferramentas de segurança existentes não são capazes de garantir o respeito às políticas de segurança existentes.**
5. **Comum o vazamento acidental de informações pela falta de cuidado de funcionários (conversa em local público, engenharia social, etc.), o que tem afetado a imagem da empresa no mercado.**

Eles acham que implementando o software de DLP, problemas de vazamento de informação estarão resolvidos. Querem sua consultoria para a melhor implantação da ferramenta possível. Quais seriam suas recomendações para a empresa?

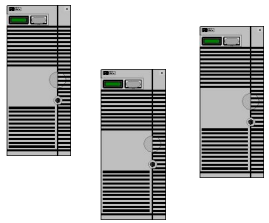
# Cenário 2

Em outra empresa, você foi contratado para ajudar a diagnosticar problemas com a implementação de uma ferramenta de DLP. A empresa sofre com um histórico recente de vazamentos de informação confidencial, mesmo contando com o DLP e com as salvaguardas:

- ✓ Políticas, Normas, Procedimentos, Padrões;
- ✓ Programas de Conscientização;
- ✓ Termos de Confidencialidade;
- ✓ Controles de Acesso físico:
  - Portas;
  - Câmeras de vídeo;
  - Biometria
  - Registros de Entrada e Saída;
  - Crachás;
- ✓ Controles de Acesso Lógicos:
  - Firewalls;
  - IDS/IPS
  - Mecanismos de Autenticação e Autorização em Sistemas.

Quais seriam as possíveis causas destes vazamentos? Qual a sua estratégia para endereçar os possíveis problemas?

# Onde a informação precisa ser Protegida por uma ferramenta de DLP?



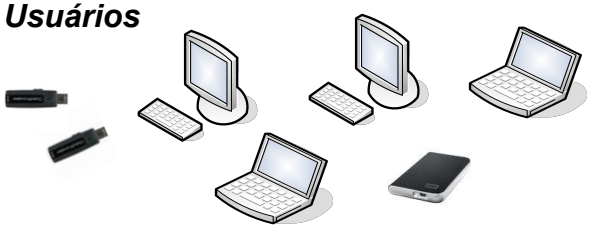
***Servidores / Pastas de Rede***

Data at Rest – Verificação de repositórios estacionários (ex.: arquivos da rede)

Data at the Endpoint – Verificação de informações armazenadas em notebooks e dispositivos portáteis (USB, CD/DVDs, etc.)

***Internet***

***Estações de Trabalho / Usuários***



Data in Motion – Verificação de informação transmitida para fora da rede da empresa (e-mail, web, etc.)

# O que precisamos para a Implementação

- Precisamos levar para a ferramenta tudo que é confidencial para o negócio daquela empresa
  - Quais níveis de classificação precisam ser incluídos?
  - Quais são as informações confidenciais para cada unidade de negócio?

- Necessário criar políticas para tratamento da informação confidencial nos diferentes e possíveis cenários.
  - Como estas informações confidenciais são transportadas, armazenadas e processadas dentro da organização?
  - Como é o fluxo de dados confidenciais?

- Necessário identificar em quais assets cada componente da solução de DLP deve ser conectado ou instalado, incluindo dispositivos de usuários, servidores de bancos de dados, storages, switches, etc.

# Já falamos disto… A ferramenta não resolve tudo

- Vazamentos não acontecem apenas no ambiente digital:
  - Impressos;
  - Informações com as pessoas;
  - Fotos;
  - Anotações.

- Vazamentos intencionais
  - Esteganografia;
  - Hacking;
  - Falta de segurança física;
  - etc.

# Por onde as empresas devem começar? Análise de Riscos!

**A organização precisa saber antes de ir adiante em um projeto de DLP:**

- ✓Quais são os agentes da ameaça para perda de dados?
- ✓Quais são os principais alvos dos atacantes (internos e externos)?
- ✓Quais tipos de elementos de dados e processos são mais comumente atacados?
- ✓Quais são os controles existentes na organização para proteger a informação?
- ✓Quais são os impactos do vazamento para os diferentes tipos de informações confidenciais?

# Por onde as empresas devem começar? Definição de Controles!

**Um Projeto de DLP não deve contemplar apenas a implantação de uma Ferramenta. É preciso também:**

- ✓Definir regras/políticas de classificação da informação;
- ✓Definir critérios para identificação da informação como "**Confidencial**" (política de classificação da informação);
- ✓Conhecer processos críticos;
- ✓Conhecer repositórios de dados e/ou bancos de dados com informações confidenciais da organização;
- ✓ Identificar todos os cenários de vazamento de informação;
- ✓Avaliar se todas as salvaguardas necessárias estão '*in-place*", incluindo a adoção de uma ferramenta de Data Loss Prevention (DLP);
- ✓Eliminar toda aquela informação que não é importante para os negócios.

# PROCESSO DE DLP

# A Prevenção de Vazamento de Informação também deve ser vista como um Processo


- Analisar Riscos
- Analisar informação confidencial (local, processos, etc.)
- Analisar Alvos de Vazamento
- Documentar Requisitos

- Avaliar soluções disponíveis
- Definir controles necessários
- Fazer análise de custo-benefício
- Finalizar solução desejada

- Criar projeto de DLP, incluindo seleção de ferramenta de DLP específica e das demais soluções necessárias
- Criar modelo de governança para a prevenção de perda de dados, políticas e processos para DLP

- Implantar ferramentas para a proteção da informação
- Parametrizar ferramenta de DLP
- Definir políticas/regras
- Desenvolver todos os controles de suporte

- Monitorar eventos com base nas políticas iniciais
- Analisar falsos positivos
- Refinar políticas e parâmetros para "information discovery"
- Testar processo de resposta a incidentes
- Ir para o estágio de bloqueio ativo para tentativas de vazamento

- Monitorar eventos e agir quando necessário
- Melhorar processos e controles para prevenção de perda de dados
- Assegurar conscientização e treinamento dos usuários