Rialide-BR

Gestão de Segurança da Informação

Felipe Curty do Rego Pinto

Quem sou?

- Coordenador de SI - BNDES
- Formação
  - Mestre em Engenharia de Software – COPPE
  - MBA Executivo – COPPEAD
  - Engenheiro Eletrônico e de Computação - UFRJ

A Equipe de SI do BNDES

Área de Gestão de Riscos

Departamento de Segurança da Informação e Processos

Gerência de Segurança da Informação

Equipe

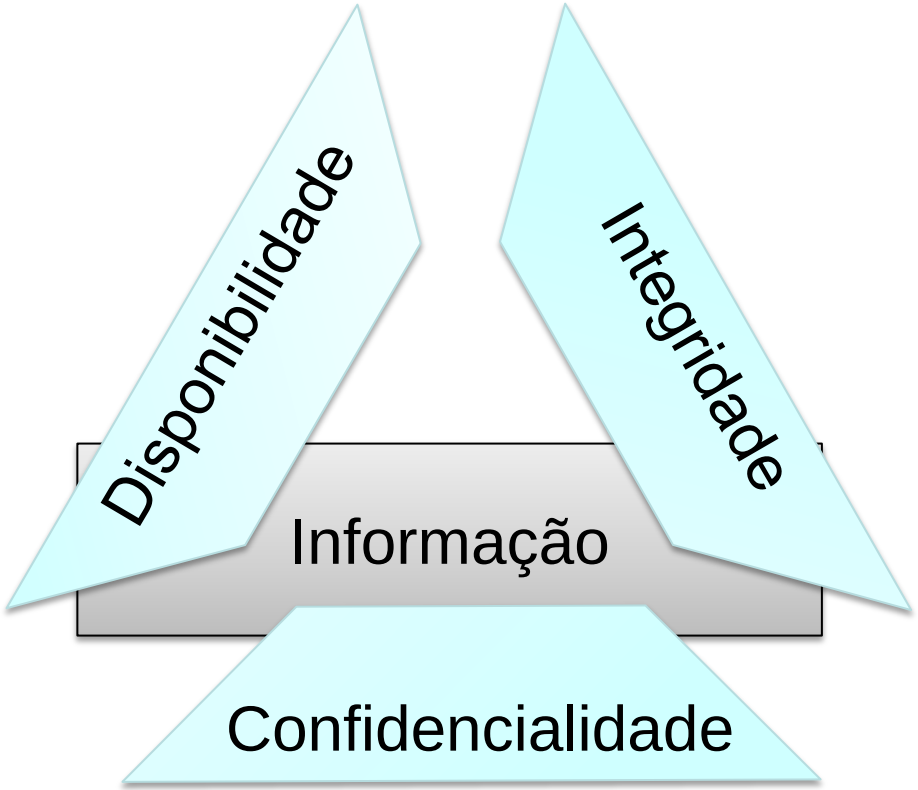
- Gerente
- Coordenador
- 4 Analistas
- 1 Estagiário

Segurança é Responsabilidade

de TODOS

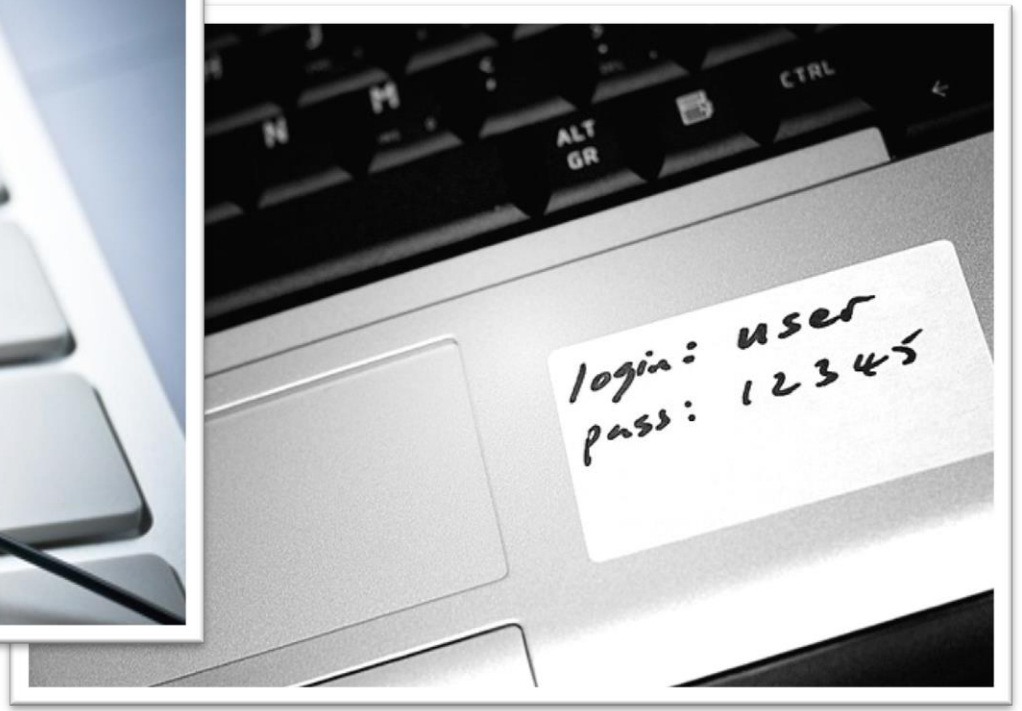
O que é Segurança da Informação?

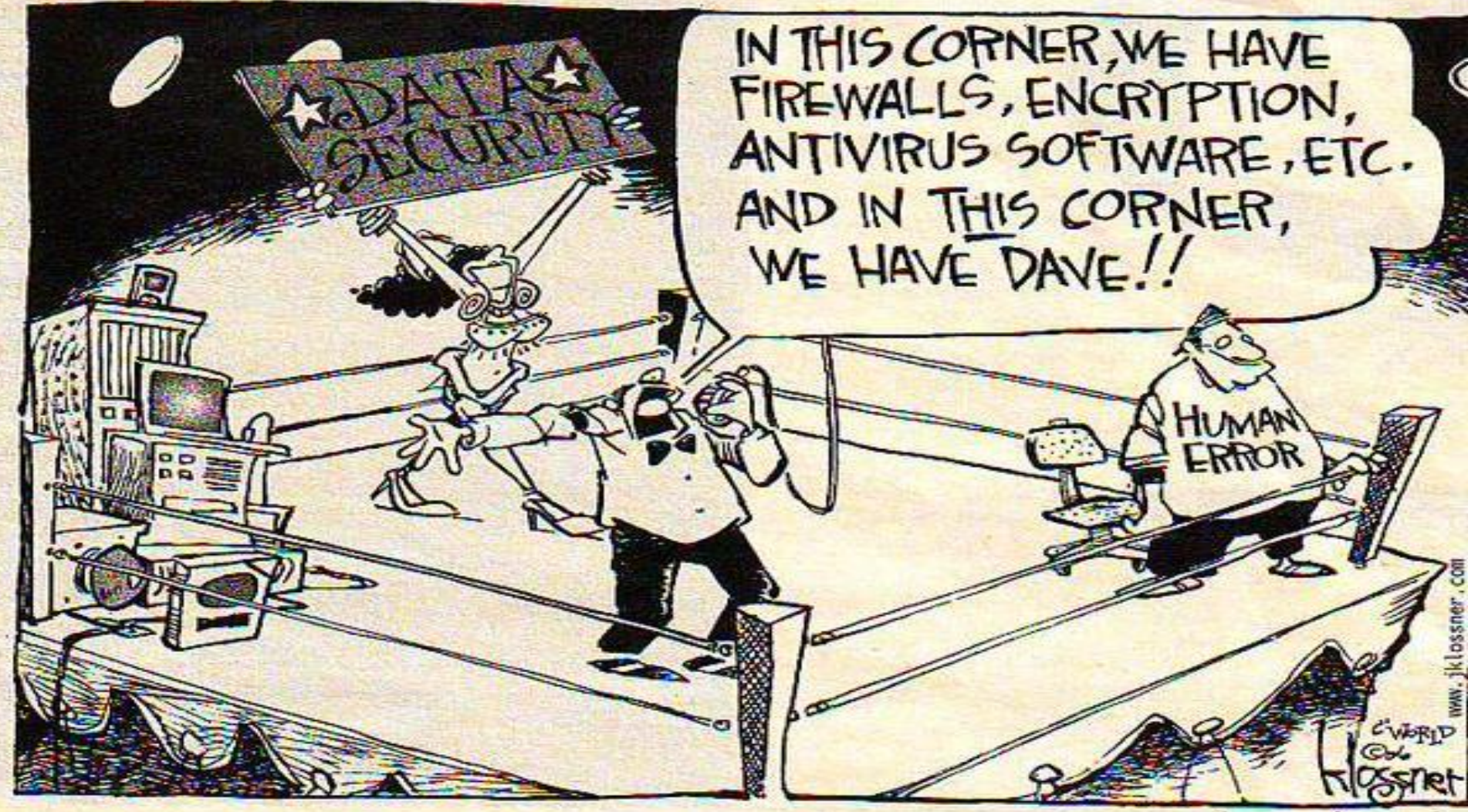
O que é Segurança da Informação?



SI envolve TECNOLOGIA

SI envolve PESSOAS




DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC.
AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklassner.com

BIZ & IT —

Bank-fraud malware not detected by any AV hosted in Chrome Web Store. Twice

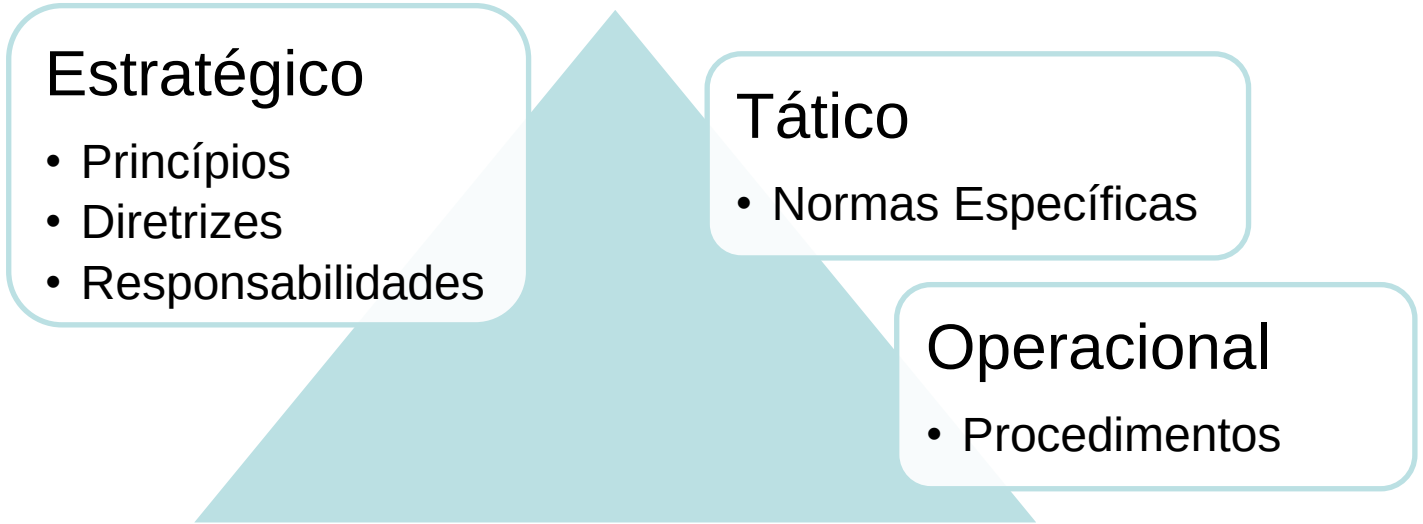
Extension that surreptitiously steals bank passwords uploaded twice in 17 days.

DAN GOODIN - 8/16/2017, 4:04 PM


VIRUS
WORD

Política de SI

- Alinhamento de como SI deve ser conduzido
- Apoio da Alta Administração



Política Corporativa de Segurança da Informação – PCSI
Responsabilidades, Diretrizes, Princípios, Atribuições e Penalidades

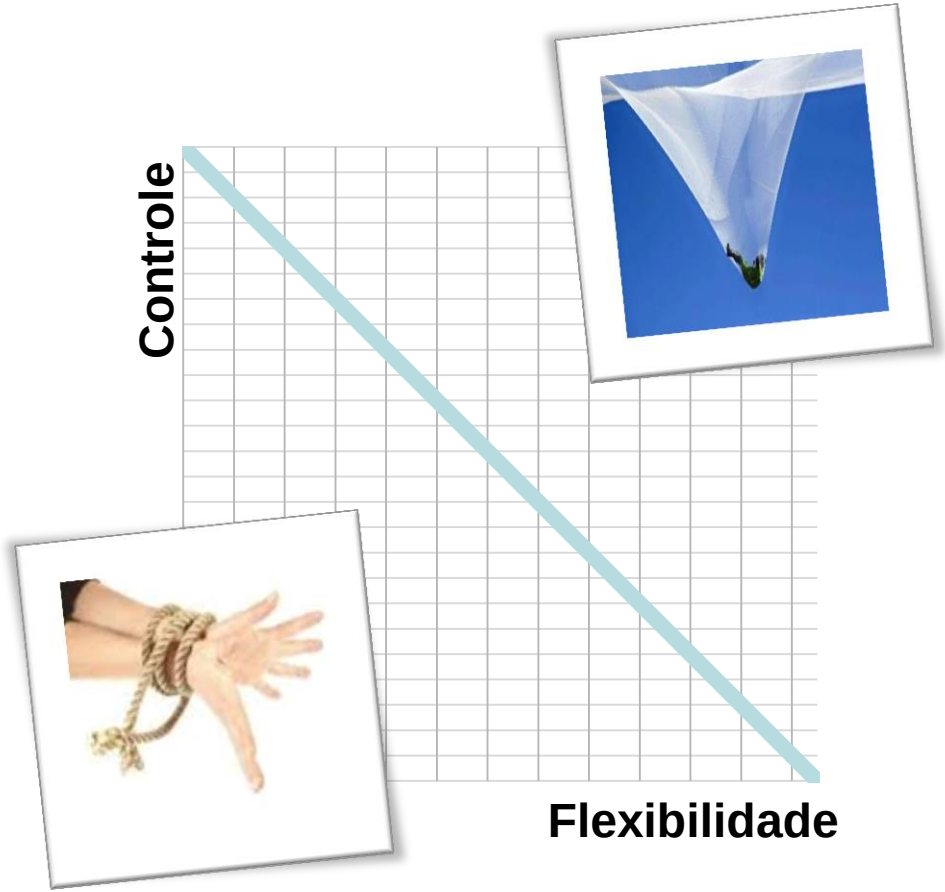
Normas

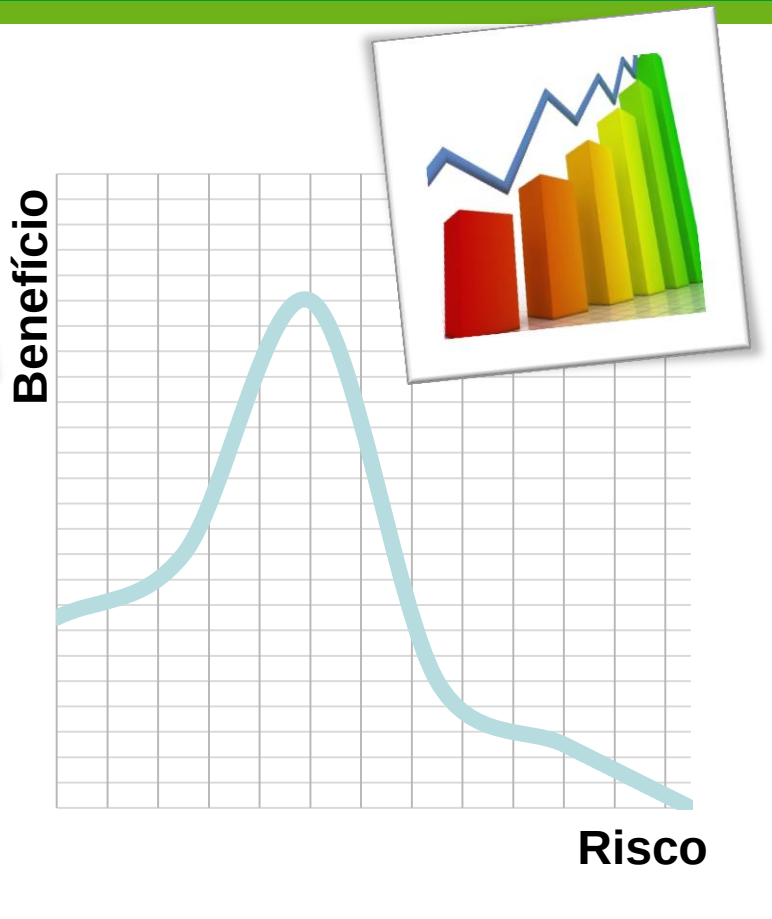
- Uso da Internet
- Uso do Correio Eletrônico
- Controle de Acesso à Informação
- Tratamento de Incidentes
- Uso de Dispositivos Pessoais
- Serviços de Computação em Nuvem
- Uso e Administração de Ativos de TI
- Acesso Remoto à Ativos de TI
- Acesso à Áreas c/ Ativos Críticos de TI
- Gestão de Vulnerabilidades

Modelos de Termo de Confidencialidade

- Contratos Administrativos
- Profissionais e Estagiários
- Empresas (sem contrato)
- Profissionais Terceirizados
- Pessoa Física (sem contrato)

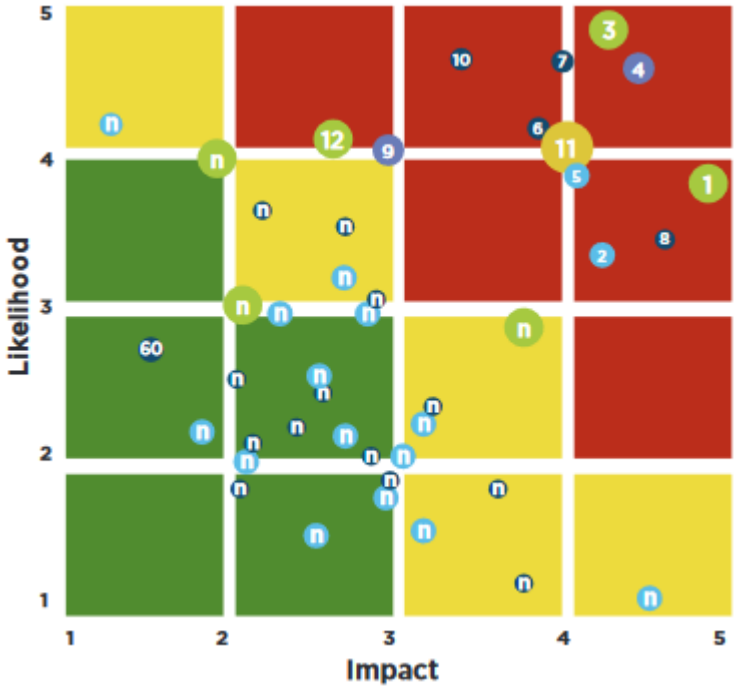
Controles e Flexibilidade





Analise de Riscos de SI

- Ponderação dos riscos, vulnerabilidade e ameaças
- Comunicação embasada com outros colaboradores
- Priorização da correção das vulnerabilidades

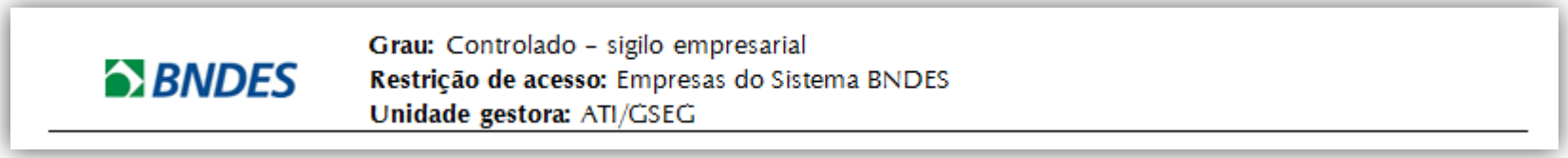


Exemplos de Controles

- Política de Senha
- Classificação da Informação
- Restrição de acesso à Internet
- Controle de Acesso ao Sistema
- Trilha de Auditoria
- Segregação de Funções
- Job Rotation
- Due Diligence

Classificação da Informação

- ABNT NBR ISO/IEC 27002:2005 – recomenda:
  - a classificação dos ativos de informação com vistas a promover o ajustado balanceamento entre gastos com controles aplicáveis e potenciais danos causados aos negócios em decorrência de eventual falha de segurança ou exposição indevida do ativo de informação; e
  - que as informações corporativas sejam classificadas para indicar a necessidade, prioridades e o nível esperado de proteção quando do tratamento da informação.



Lei de Acesso à Informação

- A publicidade é a regra e o sigilo é a exceção.
- Informações produzidas ou custodiadas pelo poder público e não classificadas como sigilosas são públicas e, portanto, acessíveis a todos os cidadãos.
  - **Exceção para hipóteses de sigilo previstas na legislação em vigor**.
- Transparência **ativa** (estrutura, repasses, despesas, licitações etc).
- Serviço de Informação ao Cidadão (**SIC**).
  - Qualquer cidadão poderá formular pedido de acesso a informações, por qualquer meio legítimo. Não é necessário indicar o motivo.

Mau uso da internet gera ação judicial

Laura Ignacio, de São Paulo
30/03/2010

Um empregado de uma empresa do setor financeiro criou um blog. E, desavisado, colocou informações sobre o balanço da companhia que, recentemente, havia aberto seu capital. O problema é que os dados eram diferentes dos enviados à Comissão de Valores Mobiliários (CVM). A empresa recebeu uma advertência formal do órgão fiscalizador e demitiu por justa causa o profissional. Cada vez mais as empresas têm enfrentado problemas devido ao mau uso da internet por seus funcionários. Muitos casos envolvem o MSN e redes sociais - Facebook, Twitter, Orkut e You Tube - e acabam gerando ações na Justiça.

O GLOBO MUNDO

BUSCAR

CAPA | PLANTÃO | MEU GLOBO | BLOGS | COLUNISTAS | EU-REPÓRTER

PAÍS | RIO | CIDADES | ECONOMIA | MUNDO | CIÊNCIA | ESPORTES | CU

Plantão | Publicada em 03/06/2009 às 16h43m

GAFE

EUA divulgam 'por engano' relatório com informações nucleares

BBC BRASIL

DÊ SEU VOTO | MÉDIA: 4,0

O governo americano divulgou por engano um detalhado relatório contendo informações sobre centenas de instalações militares do país.

O relatório, classificado como "altamente confidencial", foi publicado na internet e removido depois que a gafe foi revelada pelo jornal The New York Times - que por sua vez obteve a informação quando o site especializado em inteligência Secrecy News trouxe a notícia.

O GLOBO MUNDO

BUSCAR

CAPA | PLANTÃO | MEU GLOBO | BLOGS | COLUNISTAS | EU-REPÓRTER | O

PAÍS | RIO | CIDADES | ECONOMIA | MUNDO | CIÊNCIA | ESPORTES | CULTU

Plantão | Publicada em 18/04/2008 às 15h35m

NY: Mendigo encontra projeto confidencial para o Marco Zero no lixo

EFE

NOVA YORK - O ex-viciado e mendigo Mike Flemming, de 28 anos, encontrou cópias confidenciais do projeto arquitetônico para o Marco Zero, em Nova York, enquanto revirava lixo atrás de papelão para dormir.

Todas as páginas do plano continham a inscrição "confidencial". O projeto tinha detalhes suficientes para que terroristas planejassem um atentado aos prédios que ocuparão o lugar das Torres Gêmeas.

O mendigo disse ter ficado indignado ao encontrar o material, já que o documento poderia "ter acabado nas mãos erradas". A informação foi divulgada pelo jornal New York Post.

Ameaças Cibernéticas

Vazamento de Informação

Sigilo vazado por R$ 200

CDs com dados de aposentados e donos de carros são vendidos livremente em São Paulo

Lino Rodrigues

SÃO PAULO

Enquanto o Ministério da Justiça começa a discutir uma legislação para regulamentar a proteção de dados pessoais no Brasil, informações sigilosas que deveriam estar protegidas nos computadores do Serpro, o serviço federal de processamento de dados, do Departamento Nacional de Trânsito (Denatran) e do INSS estão sendo comercializadas livremente no centro de São Paulo. O repórter do GLOBO adquiriu por R$ 200 dois CDs com dados completos de aposentados da Previdência Social (CPF, número do benefício, endereço, telefone) e do Denatran contendo informações de milhares de proprietários de veículos em todo o país. O vendedor ofereceu ainda, pelo mesmo valor, os dados de correntistas das regiões Sul e Sudeste do banco Itaú Unibanco.

O diretor-presidente do Denatran, Alfredo Peres da Silva, disse que os funcionários do órgão não têm acesso à totalidade do banco de dados, mas apenas a determinadas informações de veículos e seus proprietários quando necessário para alguma investigação. Silva admitiu que recebeu recentemente denúncia de que uma listagem com dados de automóveis (ano 2008, modelo 2009) estava sendo vendida em São Paulo

Eliária Andrade

A lista sigilosa das UPPs

Servidor da prefeitura divulga locais das próximas unidades, guardados a sete chaves

Ana Cláudia Costa e Luiz Ernesto Magalhães

Um dos segredos mais bem guardados pelas autoridades de Segurança Pública do Rio — a localização das próximas Unidades de Polícia Pacificadoras (UPPs) — veio à tona no fim da tarde de quarta-feira durante o Fórum Urbano Mundial, organizado pela ONU Habitat na Zona Portuária. Sem perceber a presença de jornalistas na sala, o secretário-executivo da prefeitura do Rio para o Programa Nacional de Segurança Pública com Cidadania (Pronasci) do Ministério da Justiça divulgou para uma plateia formada basicamente por estrangeiros uma lista com os nomes das favelas. O prefeito Eduardo Paes desautorizou o servidor e disse desconhecer as áreas que ganharão unidades.

O documento foi exibido por menos de 30 segundos em power-point levado por Ricardo Rotemberg. Os repórteres da Rádio CBN e da Agência Brasil, que estavam na sala, conseguiram anotar que constavam na lista os morros da Providência (em fase de ocupação, no Santo Cristo), São Carlos (Estácio), Cerro-Corá (Cosme Velho), Prazeres, Fogueteiro e Fallet.

O MAPA DA PACIFICAÇÃO

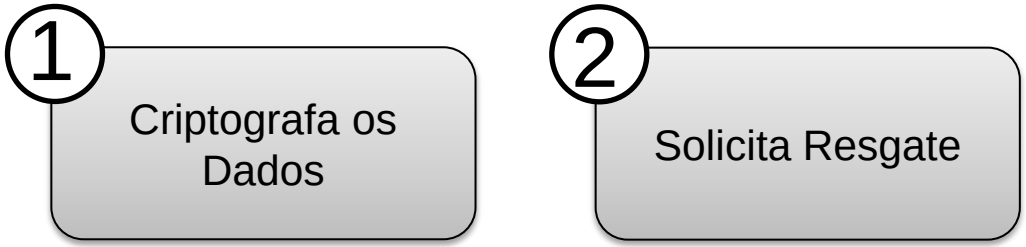
Negação de Serviço - DoS

Negação de Serviço - DoS

RAT – Remote Access Trojan

RANSOMware

RESGATE>> SEQUESTRO DE DADOS



Fotos
Documentos
Backups
...

Tempo
BitCoin


CryptoLocker
Your personal files are encrypted!
Your important files encryption produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.
Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt the files you need to obtain the private key.
The single copy of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will destroy the key after a time specified in this window. After that, nobody and never will be able to restore files...
To obtain the private key for this computer, which will automatically decrypt files, you need to pay 300 USD / 300 EUR / similar amount in another currency.
Click «Next» to select the method of payment.
Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.
Next >>
Private key will be destroyed on
12/1/2013
10:18 AM
Time left
42 : 48 : 44
Microsoft Keyboard
VLC media player
Microsoft Mouse
Recycle Bin
October Newslet...
Fox Bend Apts (2)
Lorex Client 10
WinZip
My Computer
Malwarebytes Anti-Malware
CCleaner
Microsoft Office W...
Microsoft Works
Microsoft Office P...
Microsoft Office Ex...
Blue Moon
Microsoft Office Outl...
Malwarebytes Anti-Malware 1.75.0.1300
Database version: v2013.11.29.06
Start
CryptoLocker
3:29 PM

Pagar

Chorar

Backup

Diversas Opções com Criptografia e Gratuitas

HD Externo

Internet

Colegas

By MATT BURGESS

—

Thursday 2 February 2017

Credit **iStock / ZLuketina**

Guests staying at the four-star Romantik Seehotel Jaegerwirt can pay £368 per night for panoramic views of the surrounding lake and Austrian countryside – luxury is almost a guarantee. What guests don't expect is to be caught up in a cyberattack.

At the beginning of the current ski season, the hotel revealed it had been hit by a ransomware attack in which hackers took over the controls of locks on guest rooms. Multiple reports stemming from *The Local* and news agency Central European News exclaimed guests at the hotel had been locked in their rooms by the cybercriminals.

Madison County computer servers compromised by ransomware

13 WTHR.COM STAFF

PUBLISHED: 11/05/16 10:45 PM EDT. UPDATED: 11/07/16 05:33 PM EST.

MADISON COUNTY, Ind. (WTHR) - Madison County's computer servers have been compromised by a cyber attack.

Ransomware rendered their systems inaccessible, according to Indiana State Police Capt. Dave Bursten.

Capt. Bursten emphasized to WTHR.com the attack has not endangered public safety. If you call for an ambulance or police officer, they will respond.

"It's like when I came on in the 80s - we're doing everything with pencil and paper," he explained.

Boleto Falso

[redacted] | 341-7 | 34191.75009 01544.841545 78554.760005 4 25230000093423

Local de Pagamento Pagável em qualquer agência bancária.					Vencimento 03/09/2004
Cedente Fábrica de Materiais LTDA					Agência / Código Cedente 1547/85547-5
Data do documento 20/02/2015	No documento 1234	Espécie doc. DM	Aceite N	Data processamento 20/02/2015	Nosso Número 175/00015448-4
Uso do Banco	Carteira 175	Espécie R$	Quantidade	Valor	Valor Documento 934,23
Instruções (Texto de responsabilidade do Cedente) Não receber após o vencimento Aqui entram as instruções					(-) Desconto / Abatimentos (-) Outras deduções (+) Mora / Multa (+) Outros acréscimos (=) Valor cobrado
Sacado Cléber Machado dos Santos Rua Teste do Seu Cliente [redacted]					Cód. Baixa

Autenticação Mecânica - Ficha de Compensação

Perguntas?

Felipe Curty do Rego Pinto
felipecrp@bndes.gov.br