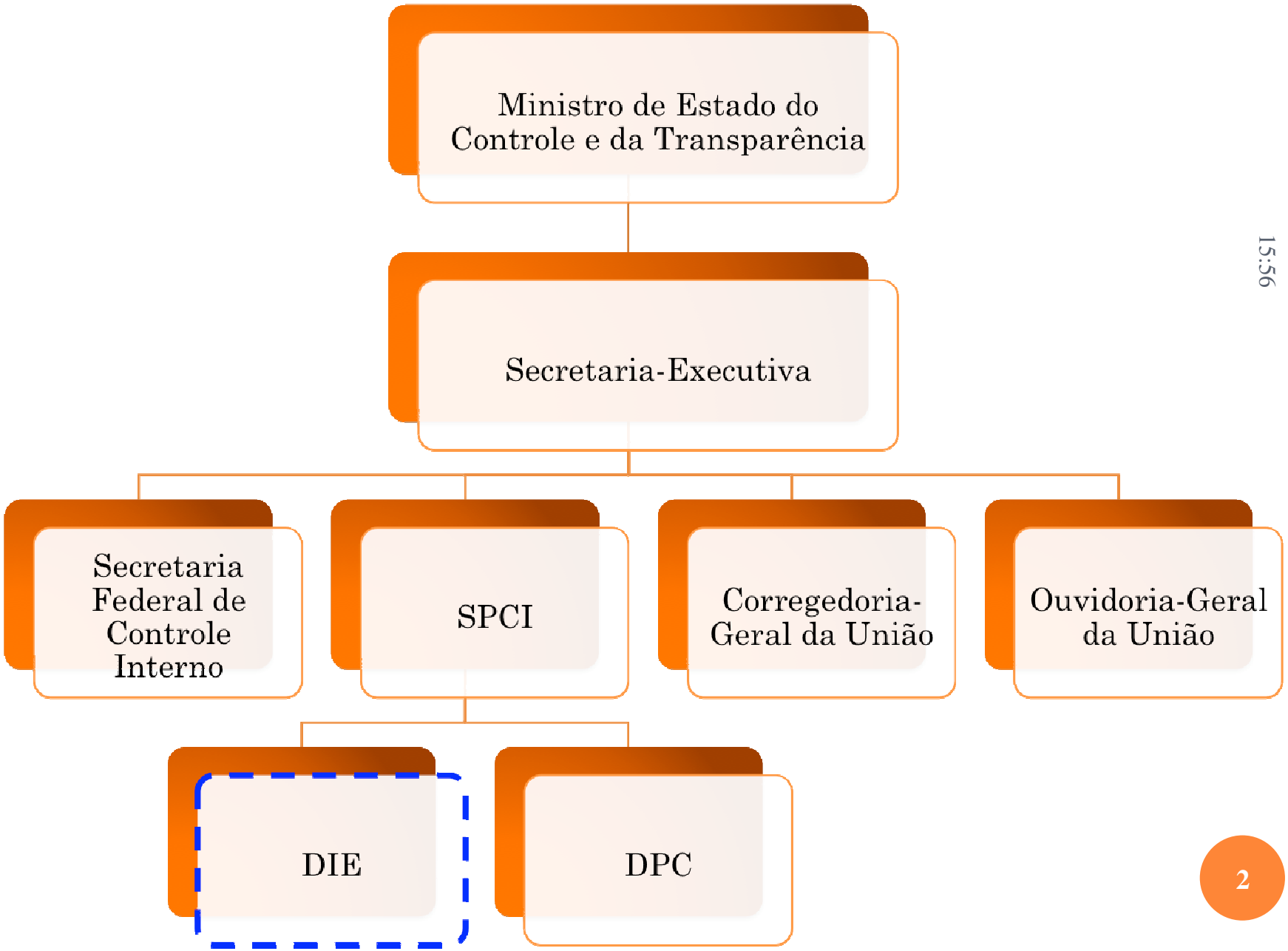
3° CURSO DE APERFEIÇOAMENTO EM OUVIDORIA PÚBLICA NATAL/RN

Segurança da Informação


Ministro de Estado do Controle e da Transparência
Secretaria-Executiva
Secretaria Federal de Controle Interno
SPCI
Corregedoria-Geral da União
Ouvidoria-Geral da União
DIE
DPC

COMPETÊNCIAS DA DIRETORIA DE INFORMAÇÕES ESTRATÉGICAS

- produzir informações e conhecimentos estratégicos que possam subsidiar as atividades das demais unidades da Controladoria-Geral da União;

- propor e adotar medidas, em articulação com a Diretoria de Sistemas e Informação, que protejam a Controladoria-Geral da União contra a disseminação não autorizada de conhecimentos e informações sigilosas ou estratégicas; e

- atuar na prevenção e neutralização das ações de inteligência adversa.

SEGURANÇA

SEGURANÇA

- Segurança é a condição de se estar protegido contra perdas ou danos.
- Risco é o evento possível, que pode causar perdas ou danos.
- Ameaça é aquilo que dá início a um evento de risco.
- Contramedida ou controle: forma de impedir que uma ameaça inicie um evento de risco.

SEGURANÇA

- Manutenção da segurança é uma tarefa de esforços assimétricos: quem defende deve defender todos os pontos – enquanto que para o agressor é suficiente identificar e focar em um ponto fraco.

"Uma corrente não é mais forte do que o seu elo mais fraco".

“Uma corrente não é mais forte do que o seu elo mais fraco”.

SEGURANÇA CORPORATIVA

- Garantir funcionamento normal
- Minimizar perdas e danos

- Corporação:

  Pessoas

  Materiais

  Informações

SEGURANÇA CORPORATIVA

- Segurança quanto às Pessoas
- Segurança quanto à Documentação e ao Material
- Segurança das Comunicações
- Segurança das Áreas
- Segurança da Informação

SEGURANÇA DA INFORMAÇÃO

SEGURANÇA CORPORATIVA

- Estamos na era do conhecimento.
- Informação é um bem valioso, mas intangível.
- Segurança da informação é diferente de segurança da informática.

Conceito de Informação

- Dados são símbolos com uma certa sintaxe;
- Informação é dados com uma certa semântica;
- Efeito/objetivo da informação é aumentar o conhecimento de determinado sujeito;
- Dado → Informação → Conhecimento

Sociedade da Informação

- Informação como fator de produção e como produto
- Informação como qualidade de um produto (design, inovação)
- Empresas e P&D
- "Capital Intangível"

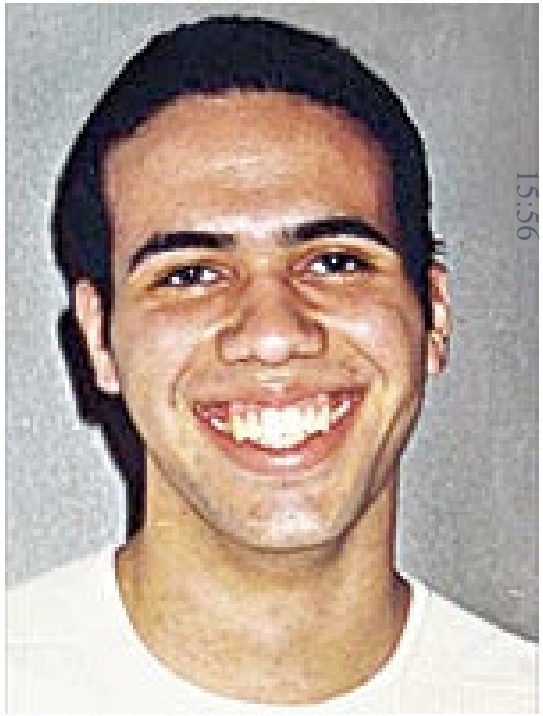

14 12:02 14


Collocation
Max Jack
CD-RW
15:56
14 12:03


15:56
Intranet PC
14 12:04


14 12:27

Reprodução/Polícia Federal/AE



George Moreira Filho: estagiário, desviou cerca de R$ 3 milhões

▪ COMENTE A REPORTAGEM

George, o golpista do INSS

Carrões blindados, lipoaspiração e até governanta. Conheça a fúria perdulária do garoto de 18 anos que fraudou o INSS

POR LÉLIAN CUNHA

Da sala no prédio da Polícia Federal em São Paulo, onde esteve sob custódia por dez dias, o primeiranista de Direito e ex-estagiário da Previdência Social mandou o recado: "Dou entrevista desde que me paguem R$ 150 mil". Diante de tamanha petulância, seu advogado, Rubens Simões, ficou perturbado. "Ele é muito deslumbrado. Esperto por um lado, bobo por outro." Filho de uma advogada e um militar da reserva, George Waldemiro Moreira Filho, 18 anos, foi preso no último dia 29, após a força tarefa da Delegacia de Repressão a Crimes Previdenciários comprovar denúncia anônima feita contra ele. De março de 2003 até o final de novembro, George desviou R$ 3 milhões do INSS para sua carteira. Duas coisas nesse caso deixam o contribuinte de cabelo em pé: a fúria perdulária do garoto e a facilidade com que se pode sangrar a Previdência.

14/02/2008 - 11h33

Petrobras confirma furto de informações sigilosas

CIRILO JUNIOR
da **Folha Online**, no Rio

Atualizada às 13h32

A Petrobras confirmou nesta quinta-feira que dados sobre pesquisas sísmicas, que podem incluir a descoberta de petróleo e gás, foram furtados de um contêiner da empresa. Segundo a estatal, as informações eram sigilosas e relevantes. A Petrobras informou apenas que o furto foi feito de uma empresa terceirizada prestadora de serviços, mas não citou nomes. Segundo fontes ouvidas pela **Folha Online**, o contêiner era transportado pela norte-americana Halliburton.

Segundo a Petrobras, o furto ocorreu no início deste mês e a investigação está sob sigilo. Uma missão especial da Polícia Federal no Rio, em conexão direta com o comando da PF em Brasília, estaria no caso.

Na ocasião do crime, o contêiner da Halliburton se dirigia a Macaé (RJ), rumo à base de operações da estatal na Bacia de Campos, transportando equipamentos, quando ocorreu o furto dos dados, que estariam em um disco rígido e computadores portáteis.

A estatal não informou detalhes sobre o conteúdo dos dados roubados, nem se continham números sobre o megacampo de Tupi, na Bacia de Santos. A Petrobras também evitou comentar detalhes do furto, mas disse que possui cópias das informações.

A Halliburton é uma das principais empresas prestadoras de serviços para o setor petrolífero do mundo e teve como um de seus executivos o vice-presidente dos Estados Unidos, Dick Cheney.

PARA VOCÊ...

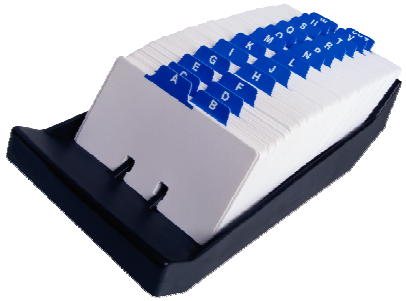
Quais informaçoes tem mais valor pessoal?

Você se preocupa em protegê-las?

PARA SUA INSTITUIÇÃO...

- Quais informações tem mais valor?
- Sua organização se preocupa em protegê-las?
- Quais os impactos em não protegê-las? (sociedade, governo, país)

ONDE ESTÁ A INFORMAÇÃO?



SEGURANÇA DA INFORMAÇÃO

Proteção dos sistemas de informação contra
- a negação de serviço a usuários autorizados,
- a intrusão, e
- a modificação desautorizada de dados ou informações,

armazenados, *em trânsito*, *em processamento*

abrangendo, inclusive, a segurança
- dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional,

assim como as destinadas a *prevenir*, *detectar*, *deter* e *documentar*

eventuais ameaças a seu desenvolvimento.

15:56

Decreto 3.505, Política de Segurança da Informação na APF

Associação Brasileira de Normas Técnicas (ABNT).

- **ISO/IEC 17799:2005**. Tecnologia da informação – Técnicas de Segurança - Código de prática para a gestão da Segurança da Informação.
- **ISO/IEC 27001:2006.** Tecnologia da informação – Técnicas de Segurança - Sistema de Gestão de Segurança da Informação - Requisitos.

SEGURANÇA DA INFORMAÇÃO

É a proteção das informações dos diversos tipos de ameaças para

garantir a continuidade do negócio,
minimizar o risco ao negócio,
maximizar o retorno sobre os investimentos e as oportunidades de negócio.

15:56

ABNT NBR ISO/IEC 17799:2005 (27002)
Código de prática para a gestão da segurança da informação

OBJETIVOS

- DISPONIBILIDADE
  - garantir que a informação, os sistemas e os ativos possam ser acessados sempre que necessário por usuários autorizados

- CONFIDENCIALIDADE
  - garantir que a informação, os sistemas e os ativos sejam acessados somente por usuários autorizados

OBJETIVOS

- INTEGRIDADE
  - garantir que a informação, os sistemas e os ativos sejam alterados somente por usuários autorizados, preservando sua exatidão e completeza

- AUTENTICIDADE
  - garantir que a informação, os sistemas e os ativos sejam genuínos e possam ser verificados quanto a sua confiança
  - garantir a veracidade do emissor/objeto/destinatário

DICA?

- Funcionários conversando em voz alta no aeroporto sobre a nova proposta de contrato
- Fogo
- Hackers
- Arquivo corrompido
- Paralisação do serviço
- Uso da Internet sem proteção
- Alteração inadequada por usuário autorizado
- Acesso não autorizado de terceiros
- Impressora no corredor

POLÍTICA DE SEGURANÇA

Política de Segurança Corporativa

- É um documento
  - Tem que estar escrita!
- Contém orientações gerais
  - Não é o lugar para detalhes
- Todos devem conhecê-la
- Deve tratar de:
  - Conscientização
  - Responsabilidades
  - Punições
- Deve ser revisada anualmente

15:56

DECRETO 3.505/2000

- Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal

- Institui também o Comitê Gestor da Segurança da Informação, coordenado pelo GSI/PR e do qual a CGU é integrante

NORMAS DECORRENTES DA POLÍTICA

- Segurança física de instalações
- Criação e manutenção de contas e senhas
- Instalação e configuração de aplicações
- Controle de acesso lógico
- Uso de Internet
- Uso de Correio Eletrônico
- Privacidade
- .....

CLASSIFICAÇÃO DE INFORMAÇÕES

- A informação deve ser classificada segundo o grau de sigilo
- Estruturar melhor a sua proteção
- A classificação deve valer tanto no ambiente computacional quanto no convencional
- Os usuários devem ser treinados em como classificar a informação sob sua responsabilidade

DECRETO 4.553/2002

- Estabelece classificação para as informações segundo grau de sigilo
  - ultra-secretos, secretos, confidenciais e reservados (+ ostensivos)
- Necessidade de conhecer
  - condição pessoal, inerente ao efetivo exercício de cargo, função, emprego ou atividade, indispensável para que uma pessoa possuidora de credencial de segurança, tenha acesso a dados ou informações sigilosos

GESTÃO DE RISCOS

GESTÃO DE RISCOS

- Atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos (ISO GUIA73)
- O que é risco?
  - Perigo ou possibilidade de perigo
  - Possibilidade de perda ou exposição à perda (GARTNER)
  - Combinação da probabilidade de um evento e a sua conseqüência (ISO GUIA 73)
  - É a probabilidade que ameaças explorem vulnerabilidades dos ativos, gerando impacto e perdas nos negócios.

AMEAÇA

- Causa potencial de um incidente que pode resultar em dano para o sistema ou organização (BS7799-3)
- O que tem potencial para causar perda e dano

- *Falha de energia, inundação, erro, empregado descontente*

VULNERABILIDADE

- Fraqueza de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças (BS7799-3)
- uma fraqueza que pode ser explorada

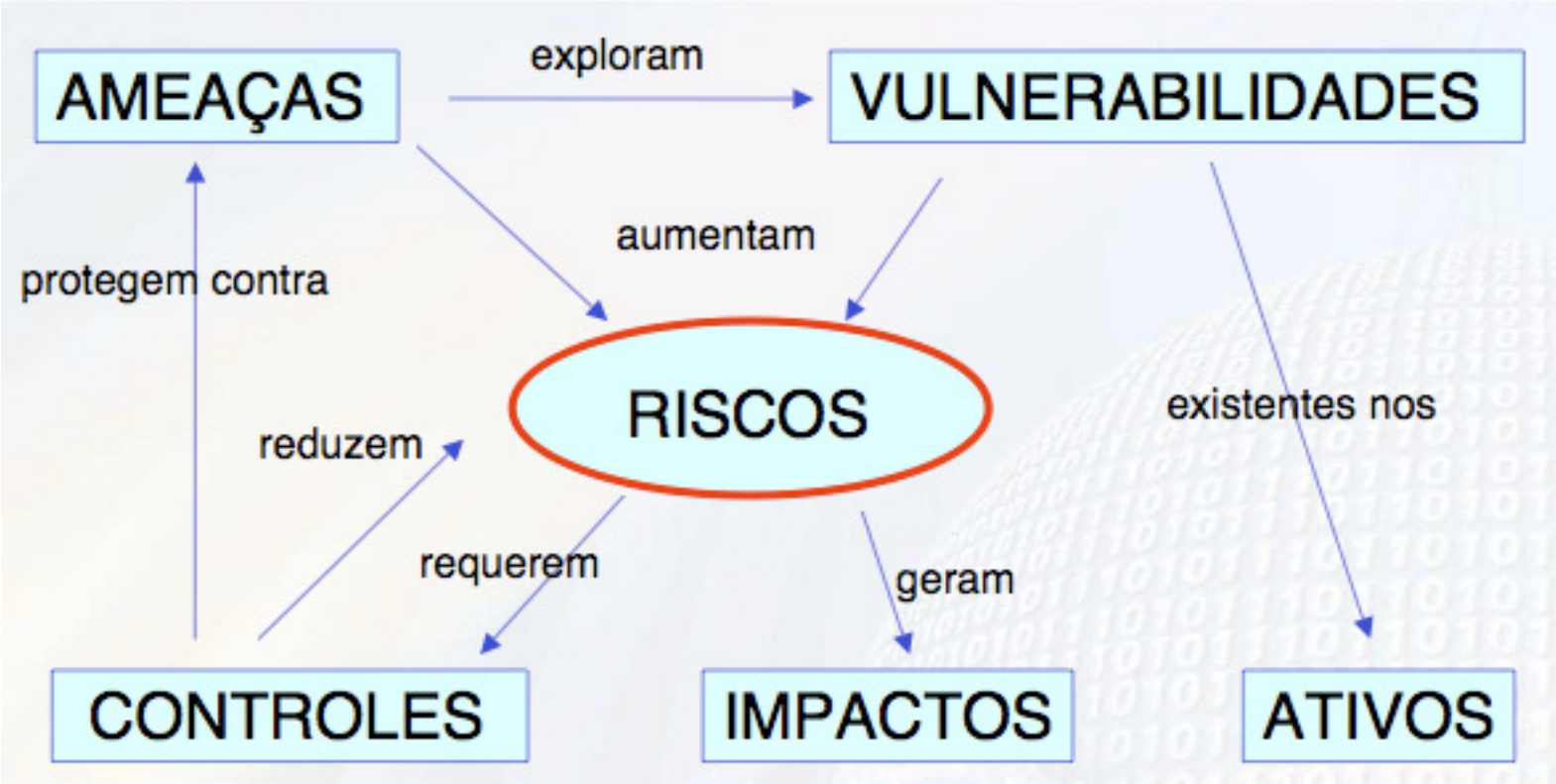
- *Política desatualizada, falta de termo de confidencialidade, falta de inventário de ativos, senhas fracas, falta de cópia de segurança*

OUTROS COMPONENTES

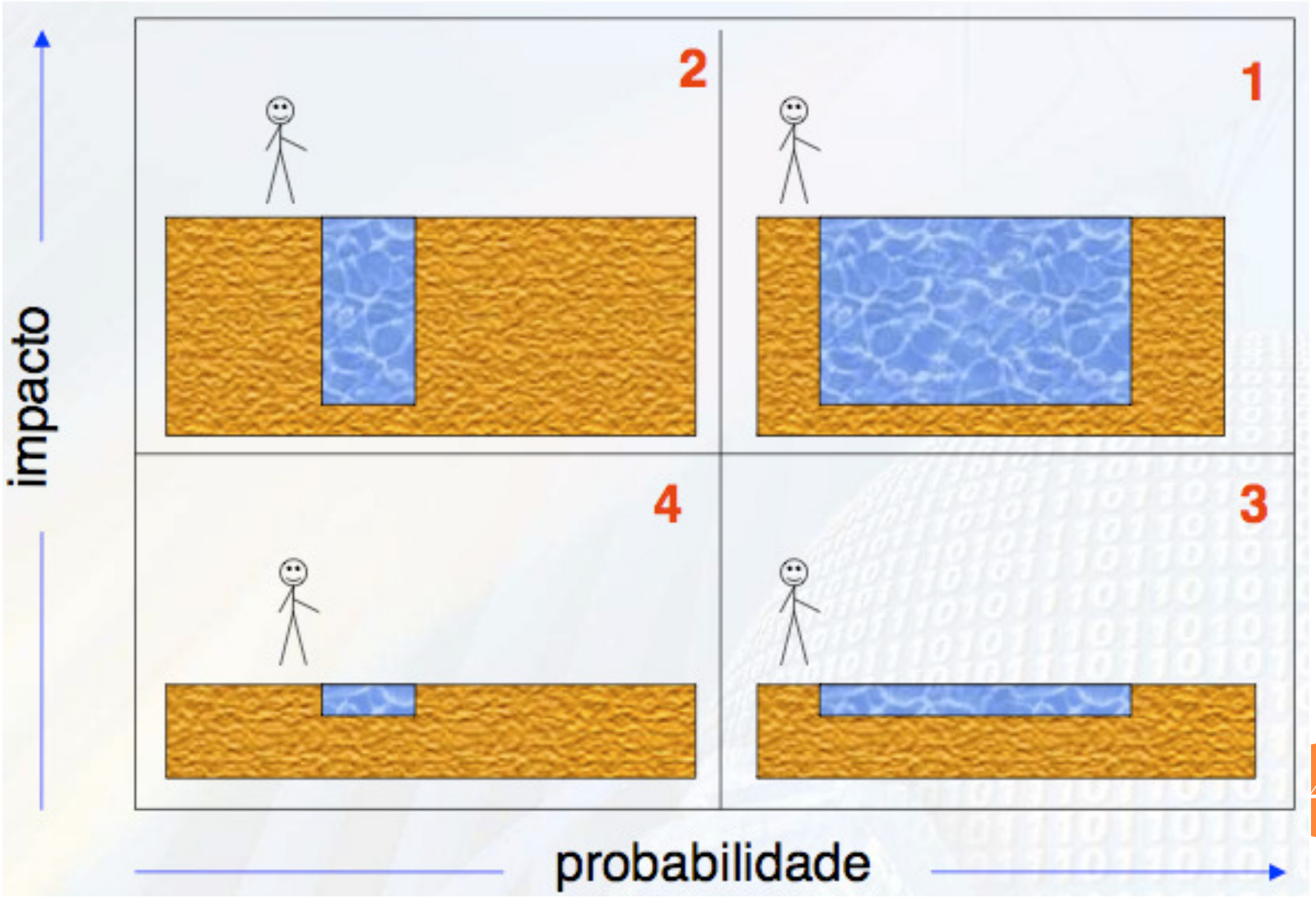
- Ativo
  - Recurso que suporta um processo, que tem valor e requer proteção
  - qualquer coisa que tenha valor para a organização (NBR 27001)
- Evento
  - Ocorrência de um conjunto específico de circunstâncias (ISO GUIA 73)
- Controle
  - Medida que minimiza, reduz ou elimina o risco

FATORES CONTRIBUINTES DO RISCO

- Probabilidade
  - grau de possibilidade que um evento ocorra (ISO GUIA 73)
  - baseada nas ameaças e vulnerabilidades (BS7799-3)
- Impacto
  - [conseqüência (ISO GUIA 73)]
  - Resultado de um evento (ISO GUIA 73)
  - Baseado no valor do ativo (BS7799-3)
  - resultado negativo da exploração de uma vulnerabilidade


AMEAÇAS
exploram
VULNERABILIDADES
aumentam
protegem contra
RISCOS
existentes nos
reduzem
requerem
geram
CONTROLES
IMPACTOS
ATIVOS

RISCO



Gerenciamento de Riscos:

- Identificação dos Riscos
- Avaliação – Risco = probabilidade vs. impacto
- Implementação – Todas as estratégias de contramedidas ou controles classificam-se em:
  - Evitar (eliminar)
  - Controlar (mitigar)
  - Aceitar (custear)
  - Transferir (terceirizar ou fazer seguros)
- Reavaliação Periódica

ENCADEAMENTO DE RISCOS

- curto circuito (ameaça 1)

  explora

- falta de sistema detecção precoce incêndio (vulnerabilidade)

  gera

- fogo (impacto/ameaça 2)

  explora

- falta de extintor automático (vulnerabilidade)

  gera

- incêndio (impacto/ameaça 3)

  explora

- ausência de brigada, sala-cofre (vulnerabilidade)

  gera

- perda de informação (impacto final)

COMO TRATAR O RISCO

- Identificação dos riscos
- Avaliação dos riscos
- Tratamento dos riscos
- Controle dos riscos

IDENTIFICAÇÃO DOS RISCOS

- Levantamento dos ativos
  - Sistemas, hardware, software, processos, pessoal, comunicações, documentação, serviços ...
- Definição do valor dos ativos
  - Custo de aquisição, de reposição, de manutenção
- Levantamento dos riscos
  - Ameaças, vulnerabilidades, impactos, probabilidades

AVALIAÇÃO DOS RISCOS

- Transformar em valores ou níveis os fatores identificados nos levantamentos realizados
- Análise custo x benefício
- Evitar, reduzir, transferir, aceitar
- Ignorar nunca!

TRATAMENTO DOS RISCOS

- Seleção dos controles
- Adoção dos controles – plano de ação

CONTROLE DOS RISCOS

- Revisão
- Indicadores
- Avaliação
- Auditoria
- Acompanhamento

AMEAÇA, VULNERABILIDADE OU RISCO?

- Refrigeração insuficiente na sala de servidores
- Fogo
- Sabotador/Hacker
- Paralisação do serviço
- Mídias em local inadequado
- DG telefônico em local de grande circulação
- Software malicioso
- Visitante mal intencionado
- Perseguição ao servidor denunciante
- Chuva forte, enchente
- Impressora no corredor

MEDIDAS DE PROTEÇÃO

EMAIL

- Não abrir arquivos em anexo de remetentes desconhecidos
- Evite clicar em links recebidos por email. Prefira digitá-los
- Se necessitar de sigilo, criptografe a mensagem (certificado digital)
- Utilize o email particular para assuntos particulares (para sua privacidade)

CONTROLE DE ACESSO

- Senhas individuais
- Evitar senhas fracas
- Excluir perfis de acesso dos funcionários desligados
- Registrar os acessos para auditoria

ARQUIVOS

- Armazenar backup dos arquivos
- Guardar backup em local diferente
- Garantir consistência entre eles
- Efetuar testes periódicos das cópias
- Criptografar informações sigilosas
- Art. 48 (Decreto 4.553). O armazenamento de documentos sigilosos, sempre que possível, deve ser feito em mídias removíveis que podem ser guardadas com maior facilidade.

DESCARTE DE INFORMAÇÕES

- Descarte adequado de:
  - Mídias
  - Documentos
  - Áreas de compartilhamento
  - Anotações, carbonos, etc
- Notebooks, pendrives

COMPORTAMENTO

- Cuidado com a Engenharia Social
- Evitar conversas em ambientes abertos
- Mesa limpa
  - Visitas, colaboradores
- Bloqueie o computador sempre que sair de sua mesa

TERCEIROS

- Conscientizar sobre a política de segurança
- Inserir cláusula específica nos contratos (Art. 59, Decreto 4.553)
- Acordo de nível de serviço (SLA – *Service Level Agreement*)

DENÚNCIAS ANÔNIMAS

LEI 8.112/90

- Art. 144. As denúncias sobre irregularidades serão objeto de apuração, desde que contenham a identificação e o endereço do denunciante e sejam formuladas por escrito, confirmada a autenticidade.
  - Parágrafo único. Quando o fato narrado não configurar evidente infração disciplinar ou ilícito penal, a denúncia será arquivada, por falta de objeto.

LEI 8.112/90

- Art. 143. A autoridade que tiver ciência de irregularidade no serviço público é obrigada a promover a sua apuração imediata, mediante sindicância ou processo administrativo disciplinar, assegurada ao acusado ampla defesa

OFÍCIO-CIRCULAR Nº 52/2008/OGU/CGU-PR

- Nenhuma manifestação anônima pode justificar, isoladamente, a abertura de processo ou procedimento formal na unidade de Ouvidoria.
- Poderá ser adotada medida sumária informal de verificação da ocorrência do(s) fato(s) alegado(s). Encontrado elemento de verossimilhança poderá a unidade de Ouvidoria abrir o processo ou procedimento cabível.
- A manifestação anônima não deverá ser conhecida no processo ou procedimento formal da unidade de Ouvidoria (não deve ser juntada aos autos), sendo este baseado tão somente nos fatos efetivamente verificados na ação sumária realizada previamente.

MATERIAL DE CONSULTA

SEGURANÇA DA INFORMAÇÃO

- ABNT ISO/IEC 27001 – Sistema de Gestão em Segurança da Informação
- ABNT ISO/IEC 27002 – Conjunto de controles de segurança da informação
- ABNT ISO/IEC Guia 73:2005, Gestão de riscos – Vocabulário
- Manual de boas práticas em Segurança da Informação (http://www.tcu.gov.br)

Controladoria-Geral da União

Secretaria de Prevenção da Corrupção e Informações Estratégicas

Diretoria de Informações Estratégicas

15:56

Felipe Dantas

felipe.araujo@cgu.gov.br

55-61-3412-7264

http://www.cgu.gov.br