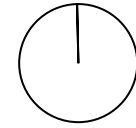




Presidência da República
Controladoria-Geral da União
Secretaria de Prevenção da Corrupção e Informações Estratégicas
Diretoria de Informações Estratégicas

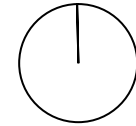


Segurança da Informação

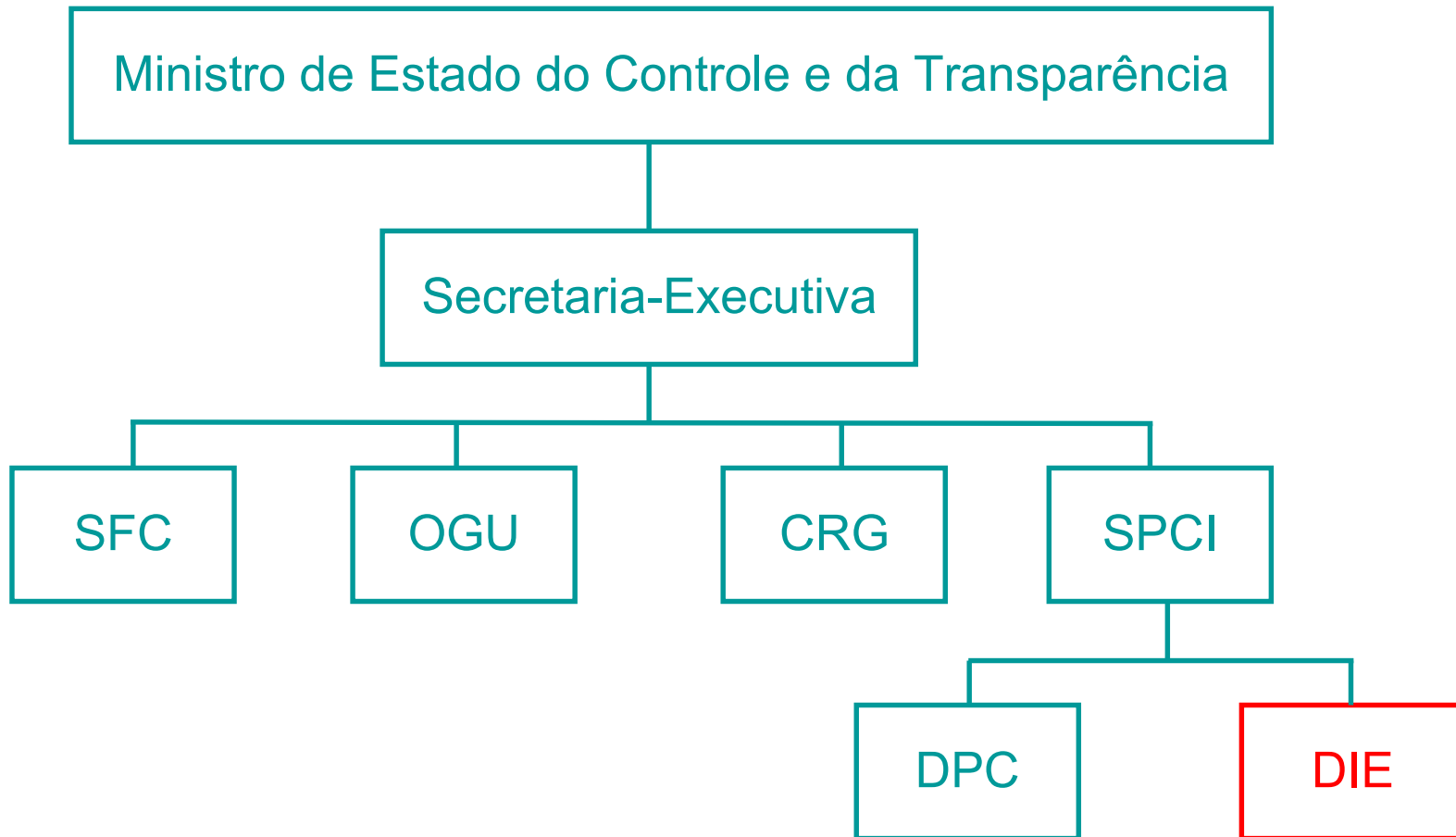
5º Curso de Aperfeiçoamento em Ouvidoria Pública

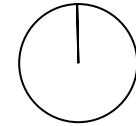
Junho de 2010

Alexandre Andrade



Controladoria-Geral da União





Sumário

- Introdução
- Definições
- Objetivos
- Gestão de Riscos
- Política de Segurança
- Medidas de Proteção



Introdução

- Sociedade da Informação
 - Aumento da vulnerabilidade e dos danos potenciais
- Segurança x (Eficiência, Conforto)
 - Aparentemente não contribui para a atividade-fim
 - Primeira área a sofrer cortes de gastos
 - Medidas sofrem resistência dos colaboradores
 - Ganha destaque quando não funciona



Introdução

- Segurança da Informação
 - Não se confunde com segurança computacional
 - Vai além da proteção ao sigilo
 - Relevante para a atividade de ouvidoria pública

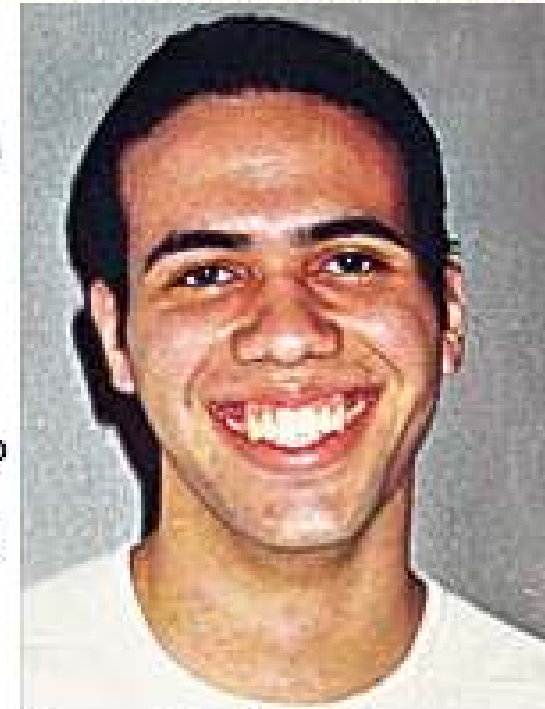


George, o golpista do INSS

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

POR LÍLIAN 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.



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

COMENTE A REPORTAGEM



14/02/2008 - 11h33

Petrobras confirma furto de informações sigilosas

CIRILO JUNIOR

da **Folha Online**, no Rio

Atualizada às 13h32

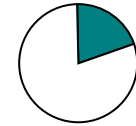
A Petrobras confirmou nesta quinta-feira que dados sobre pesquisas sísmicas, que podem incluir a descoberta de petróleo e gás, foram furtados de um contêiner da empresa. Segundo a estatal, as informações eram sigilosas e relevantes. A Petrobras informou apenas que o furto foi feito de uma empresa terceirizada 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.



Quadrilha usava informações sigilosas do INSS em golpes

comentários
3

09 de maio de 2010 • 22h48

NOTÍCIA

Uma quadrilha baseada na região de Sorocaba (SP), no interior de São Paulo, usava dados sigilosos do INSS de aposentados para aplicar golpes em seis Estados do País. Eles fabricavam documentos falsos para obtenção de empréstimos consignados. Em seis meses eles teriam obtido R\$ 2 milhões. As informações são do programa *Fantástico da TV Globo*.



As investigações da polícia duraram seis meses e resultaram na prisão de 10 integrantes da quadrilha nesta semana. O grupo comprava documentos em branco no centro de São Paulo e usava os dados da vítima com a foto de algum integrante com idade aproximada. A polícia acredita que eles conseguiam informações privilegiadas junto à previdência e instituições bancárias.

[mais notícias de polícia »](#)

Redação Terra



Segurança da Informação

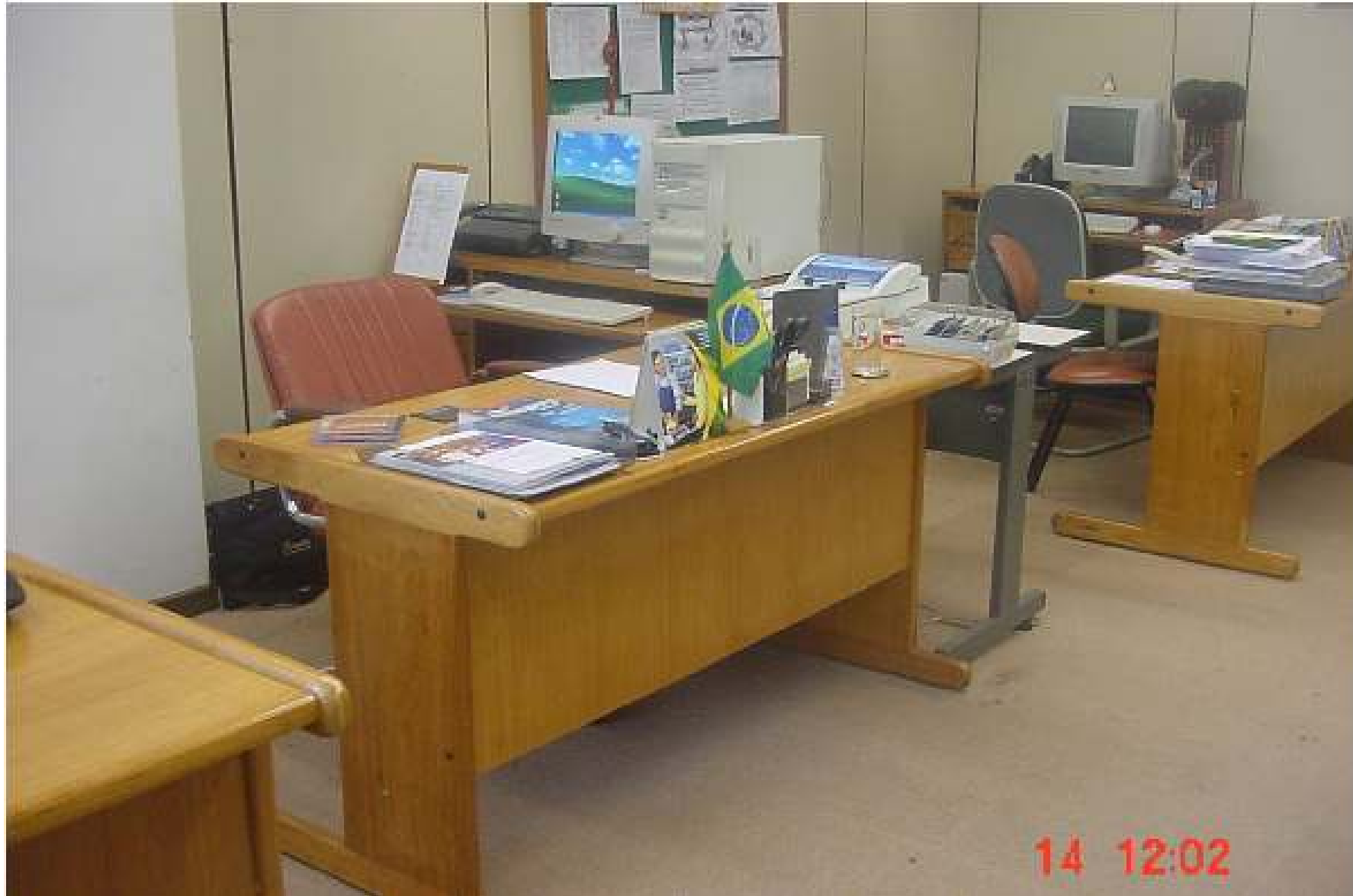
■ Pessoal



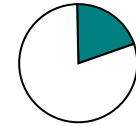
■ Institucional: mesmo cuidado?

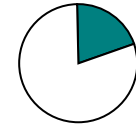


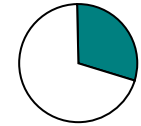
Presidência da República
Controladoria-Geral da União
Secretaria de Prevenção da Corrupção e Informações Estratégicas
Diretoria de Informações Estratégicas



14 12:02









Definições

Segurança da Informação

- Proteção dos sistemas de informação contra:
 - ◆ negação de serviço a usuários autorizados
 - ◆ intrusão
 - ◆ modificação desautorizada de dados ou informações
 - ◆ armazenadas
 - ◆ em trânsito
 - ◆ em processamento

Decreto 3.505/2000, Política de Segurança da Informação na APF



Definições

Segurança da Informação

- Abrangendo, inclusive, a segurança:
 - ◆ dos recursos humanos
 - ◆ da documentação e do material
 - ◆ das áreas
 - ◆ das comunicações
 - ◆ computacional

Decreto 3.505/2000, Política de Segurança da Informação na APF



Definições

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

ABNT NBR ISO/IEC 17799:2005 (27002)

Código de prática para a gestão da segurança da informação



Objetivos

- Garantias a serem conferidas às informações, aos sistemas e aos ativos
 - ◆ Disponibilidade
 - ◆ Integridade
 - ◆ Confidencialidade
 - ◆ Autenticidade



Objetivos

■ Disponibilidade

- ◆ Acesso aos usuários autorizados sempre que necessário
- ◆ Ausência dessa garantia pode gerar situações de negação de serviço (DoS)
 - ◆ Prejuízo em situações de urgência
 - ◆ Danos à imagem da instituição/empresa



Objetivos

■ Integridade

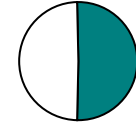
- ◆ Alteração de dados e informações apenas por usuários devidamente autorizados
- ◆ Armazenamento, processamento e transmissão dos dados e informações realizados de forma a preservar a exatidão e completeza dos registros
- ◆ Ausência dessa garantia pode gerar perda ou falsificação de dados/informações



Objetivos

■ Confidencialidade

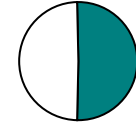
- ◆ Acesso aos dados e informações restrito aos usuários devidamente autorizados
- ◆ Proteção em todas as fases: armazenamento, transmissão e processamento
- ◆ Ausência dessa garantia pode resultar na quebra de sigilo



Objetivos

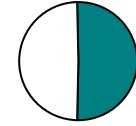
■ Autenticidade

- ◆ Certeza de que os dados/informações provêm das fontes anunciadas
- ◆ Também engloba o *não-repúdio* ou *irretratabilidade* - o usuário fica impossibilitado de negar a autoria
 - ◆ Responsabilização
- ◆ Ausência dessa garantia pode resultar no uso de informações falsas



Objetivos

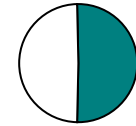
- Classificação de ameaças
 - ◆ Conversa em voz alta no aeroporto sobre a nova proposta de contrato
 - ◆ Incêndio
 - ◆ Hackers
 - ◆ CD-ROM danificado
 - ◆ Paralisação do serviço
 - ◆ Uso da Internet sem proteção
 - ◆ Alteração anônima nos dados
 - ◆ Acesso não autorizado de terceiros
 - ◆ Impressora no corredor
 - ◆ Impossibilidade temporária de acesso à Internet



Gestão de Riscos

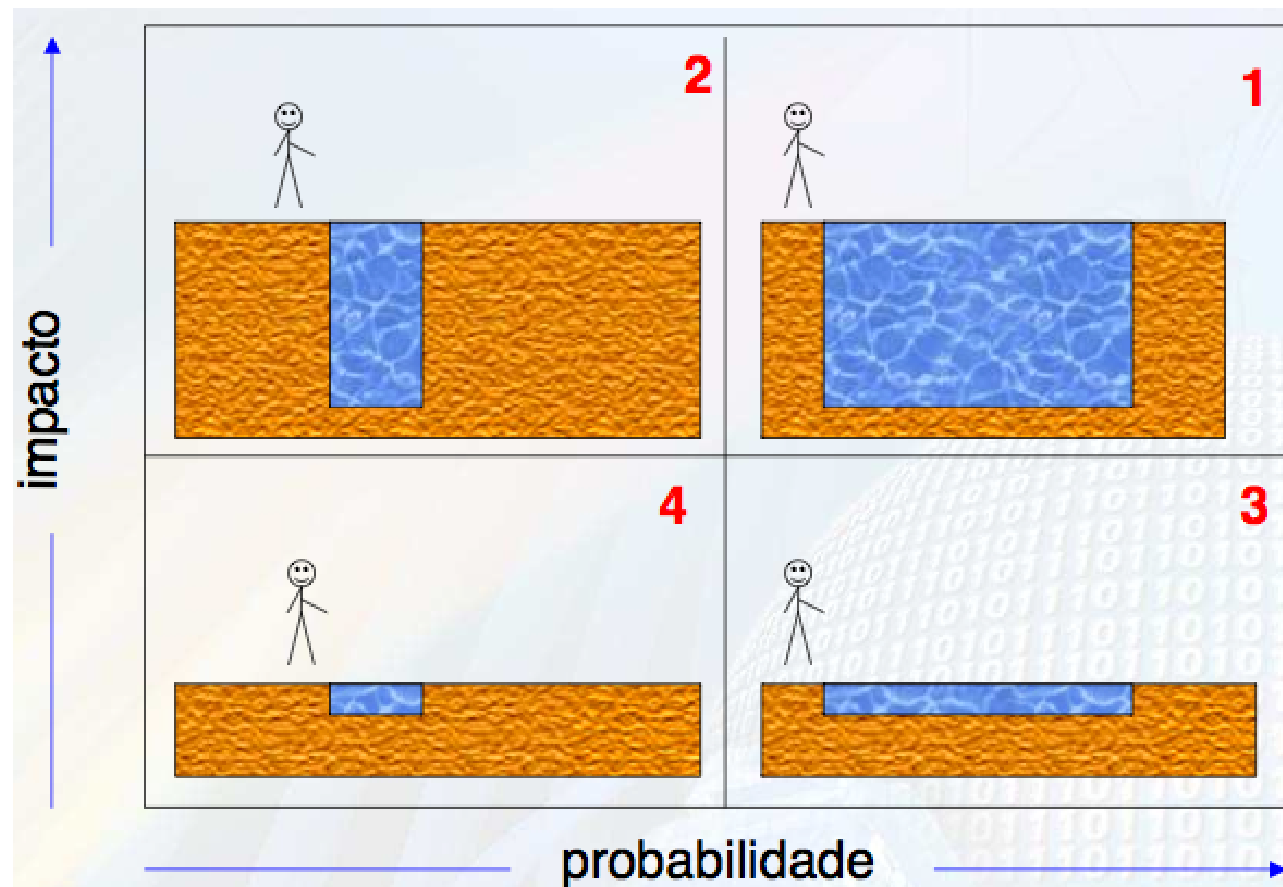
- Atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos (ABNT ISO GUIA 73:2009)

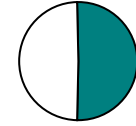
- Risco
 - ◆ Perigo ou possibilidade de perigo
 - ◆ Possibilidade de perda ou exposição à perda
 - ◆ Combinação da probabilidade de um evento e a sua consequência



Gestão de Riscos

■ Risco: Probabilidade x Impacto





Gestão de Riscos

- Gerenciando riscos
 - ◆ Identificação
 - ◆ Avaliação
 - ◆ Tratamento
 - ◆ Controle



Gestão de Riscos

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



Gestão de Riscos

- Avaliação de riscos
 - ◆ Classificação dos riscos levantados em níveis ou valores numéricos
 - ◆ Análise probabilidade x impacto



Gestão de Riscos

- Tratamento de riscos
 - ◆ Elaboração dos controles
 - ◆ Medidas de proteção
 - ◆ Análise custo x benefício
 - ◆ Evitar, reduzir, transferir, aceitar (nunca ignorar)
 - ◆ Adoção dos controles
 - ◆ Plano de ação



Gestão de Riscos

- Controle de riscos
 - ◆ Revisão periódica
 - ◆ Utilização de indicadores
 - ◆ Avaliação
 - ◆ Auditoria
 - ◆ Acompanhamento



Política de Segurança

- Descreve as regras básicas para o uso e a manipulação da informação em uma organização
- Documento escrito
- Alinhada com os objetivos do negócio
- Conhecida por todos os colaboradores
- Revisada periodicamente



Política de Segurança

- Decreto nº 3.505/2000
 - ◆ Institui a Política de Segurança da Informação nos órgãos e entidades da APF
 - ◆ Institui também o Comitê Gestor de Segurança da Informação, coordenado pelo GSI/PR, do qual a CGU é integrante
 - ◆ Documento básico: apenas 8 (oito) artigos



Política de Segurança

Política de Segurança (Regras Básicas)

Normas Específicas

- Segurança física de instalações
- Sistemas de combate a incêndio
- Acesso de colaboradores, usuários e visitantes
- Criação e manutenção de contas e senhas
- Instalação e configuração de aplicações
- Uso de internet e correio eletrônico
- Privacidade



Google

Centro de Privacidade do Google

Visão geral da Privacidade

[Política de Privacidade](#)

[Perguntas frequentes](#)

[Termos de Serviço](#)

Mais informações sobre privacidade:

[Política de Privacidade para os anúncios e a rede de conteúdo do Google](#)

[Chrome](#)

[Armazém 3D](#)

[Desktop](#)

[Documentos e Planilhas](#)

[Gmail](#)

[GOOG-411](#)

[Grupos](#)

[Mapas](#)

[Celular](#)

[Orkut](#)

[iGoogle](#)

[Pesquisa personalizada](#)

Visão geral da Privacidade do Google

Escopo

Esta declaração se aplica aos produtos, serviços e sites do Google (coletivamente chamados de "serviços" do Google). Informações pessoais e outros dados que coletamos

- O Google coleta [informações pessoais](#) quando você se cadastra em um serviço do Google e quando fornece esse tipo de informações voluntariamente. Podemos combinar as informações pessoais fornecidas por você com as informações de outros serviços do Google ou de terceiros para proporcionar ao usuário uma experiência melhor, incluindo a personalização do conteúdo para você.
- O Google usa [cookies](#) e outras tecnologias para melhorar a sua experiência on-line e para saber como você usa nossos serviços, com a finalidade de melhorar a qualidade deles.
- Os servidores do Google registram as informações automaticamente quando você visita nosso website ou quando usa algum de nossos produtos, incluindo o URL, o endereço IP, o tipo de navegador e o idioma, a data e a hora de sua solicitação.
- [Leia mais](#) na política de privacidade completa.

Usos

- Podemos usar as informações pessoais para fornecer os serviços solicitados por você, incluindo os serviços que exibem publicidade e conteúdo personalizado.
- Podemos usar as informações pessoais também para auditoria, pesquisa e análise para operar e aprimorar as tecnologias e os serviços do Google.
- Podemos compartilhar [informações não pessoais agregadas](#) com terceiros de fora do Google.
- Quando trabalhamos com terceiros para nos ajudar no processamento de suas informações pessoais, exigimos que eles cumpram com a nossa Política de Privacidade e com outras medidas adequadas de segurança e de confidencialidade .
- Podemos também compartilhar informações com terceiros em circunstâncias limitadas, incluindo a necessidade de estar de acordo com o processo legal, impedindo a fraude ou o dano iminente e garantindo a segurança de nossa rede e serviços.
- O Google processa as informações pessoais em seus servidores nos Estados Unidos da América e em outros países. Em alguns casos, processamos as informações pessoais em um servidor fora de nosso país.
- [Leia mais](#) na política de privacidade completa.



Medidas de Proteção

- Controle de acesso
- Segurança do material e das instalações
- Trânsito de documentos sigilosos
- Armazenamento de dados
- Internet e Correio Eletrônico
- Telefone
- Descarte de informações
- Colaboradores externos
- Comportamento



Medidas de Proteção

- Controle de acesso
 - ◆ Físico
 - ◆ Necessidade de identificação e registro
 - ◆ Uso de crachá
 - ◆ Horários de entrada/saída
 - ◆ ...
 - ◆ Lógico
 - ◆ Senhas individuais e fortes
 - ◆ Excluir perfis de usuários desligados
 - ◆ Registro de acessos para auditoria
 - ◆ ...



Medidas de Proteção

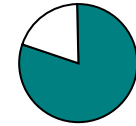
- Segurança do material e das instalações
 - ◆ Sistema de combate a incêndio
 - ◆ Sistema de vigilância
 - ◆ Manutenção das instalações
 - ◆ Controle de equipamentos eletrônicos na entrada e na saída
 - ◆ Procedimentos de trancamento e abertura de salas
 - ◆ Definição de áreas de acesso restrito



Medidas de Proteção

- Trânsito de documentos sigilosos
 - ◆ Classificação: reservado, confidencial, secreto, ultra-secreto
 - ◆ Marcação em todas as páginas
 - ◆ Acondicionamento em envelopes duplos
 - ◆ Externo: sem qualquer identificação
 - ◆ Interno: lacrado, contendo destinatário e grau de sigilo
 - ◆ Controle da reprodução

Decreto nº 4.553/2002, Salvaguarda de dados, informações, documentos e materiais sigilosos na APF



Medidas de Proteção

- Armazenamento de dados
 - ◆ Rotina de backup
 - ◆ Atualização periódica
 - ◆ Garantir a consistência
 - ◆ Testes periódicos das cópias
 - ◆ Manutenção da cópia em local diferente
 - ◆ Dados sensíveis
 - ◆ Utilizar criptografia quando necessário
 - ◆ Uso de softwares de compactação (zip,rar) com senha
 - ◆ Prover segurança também ao backup



Medidas de Proteção

■ Internet e Correio Eletrônico

- ◆ Mensagens sigilosas devem ser criptografadas ou simplesmente não enviadas
- ◆ Nunca abrir anexos de remetentes desconhecidos
- ◆ Evitar clicar em links (digitar o endereço)
- ◆ Comunicações oficiais nunca são enviadas só por e-mail
- ◆ Atenção para as informações sobre certificados digitais (“https://...”, cadeado indicado no navegador)
- ◆ Ler as mensagens e avisos, antes de clicar em OK
- ◆ Usar ao menos duas contas de e-mail (particular e profissional)
- ◆ Anti-vírus, firewall e atualização do sistema operacional



Medidas de Proteção

■ Telefone

- ◆ Evitar ao máximo tratar de assuntos sigilosos
 - ◆ Nenhum telefone é seguro
- ◆ Evitar dar o nome ao atender (aguardar a identificação do interlocutor)
- ◆ Não passar informações sensíveis no primeiro momento
 - ◆ Solicitar o telefone para contato posterior



Medidas de Proteção

- Descarte de informações
 - ◆ Uso de trituradores
 - ◆ Documentos
 - ◆ Carbono
 - ◆ Mídias
 - ◆ Arquivos eletrônicos
 - ◆ Softwares específicos para apagamento de arquivos
 - ◆ Atenção especial às pastas de compartilhamento de arquivos
 - ◆ Pen drive: apenas para trânsito de dados (deve ser mantido o mais vazio possível)



Medidas de Proteção

- Colaboradores Externos
 - ◆ Conscientizar sobre a política de segurança
 - ◆ Inserir cláusula específica nos contratos
 - ◆ Restringir o manuseio de informações sensíveis



Medidas de Proteção

■ Comportamento

- ◆ Manter a mesa “limpa”
- ◆ Bloquear o computador sempre que se ausentar
- ◆ Controle sobre os meios de impressão
- ◆ Evitar conversas sobre assuntos profissionais em ambientes abertos
- ◆ Usar o critério “necessidade de saber”



Medidas de Proteção

■ Comportamento

◆ Atenção à Engenharia Social

- ◆ Divulgação de informações em redes sociais (orkut, facebook, twitter, blogs)
- ◆ Possibilidade da exploração de características pessoais para obtenção de informações:
 - ◆ Ambição
 - ◆ Vaidade
 - ◆ Carência afetiva
 - ◆ ...



Presidência da República
Controladoria-Geral da União
Secretaria de Prevenção da Corrupção e Informações Estratégicas
Diretoria de Informações Estratégicas



Presidência da República
Controladoria-Geral da União
Secretaria de Prevenção da Corrupção e Informações Estratégicas
Diretoria de Informações Estratégicas

Alexandre Andrade Pires

alexandre.pires@cgu.gov.br

<http://www.cgu.gov.br>

<http://www.portaldatransparencia.gov.br>