SEMINÁRIO RNP
de CAPACITAÇÃO
e INOVAÇÃO - SCI

Segurança da Informação e Comunicações na APF

16º SIC 2010

CURITIBA-PR

Eduardo Wallier Vianna

CTIR Gov

AGENDA

- **APF**
- **CGTIR - CTIR Gov**
- **Ações em andamento**
- **Aspectos Jurídicos**

Ameaças e Vulnerabilidades

Ameaças e Vulnerabilidades

ADMINISTRAÇÃO PÚBLICA FEDERAL

- **39 ministérios**
- **≅ 6.000 entidades públicas**
- **926.800 servidores federais - Executivo**

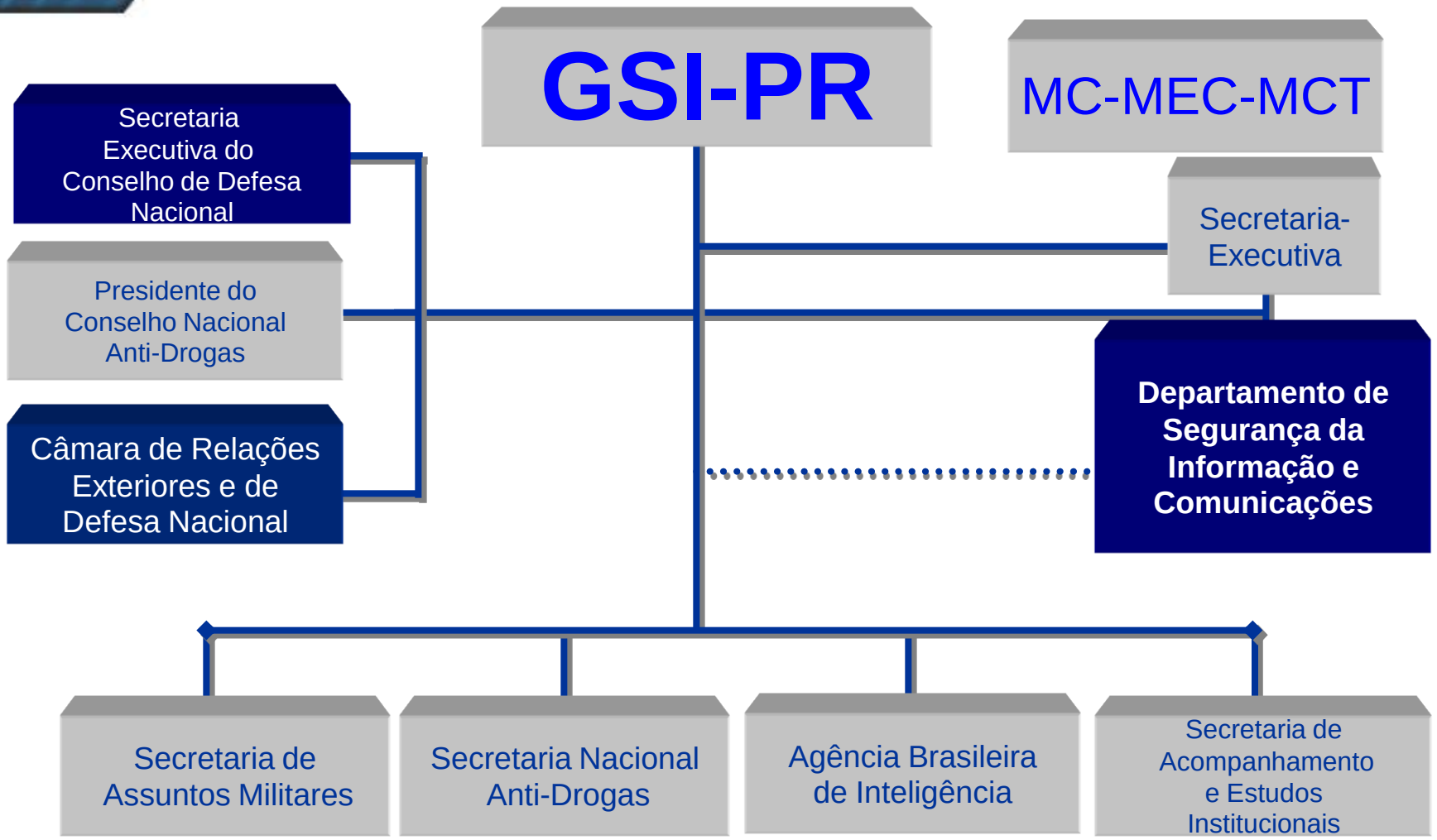
Administração direta =	225.412	Empresas Públicas=	23.036
Autarquias e Fundações=	328.217	Soc. de Economia Mista =	12.068
MPU =	8.384	Militares=	325.683

≅ 320 principais redes do governo federal

e,

- **≅ 12.000 sites .gov.br** (+ de 6 milhões páginas)

GABINETE DE SEGURANÇA INSTITUCIONAL



COMPETÊNCIAS

(Lei nº 10.683, de 29 de maio de 2003)

Coordenação da Inteligência Federal e atividades de Segurança da Informação.

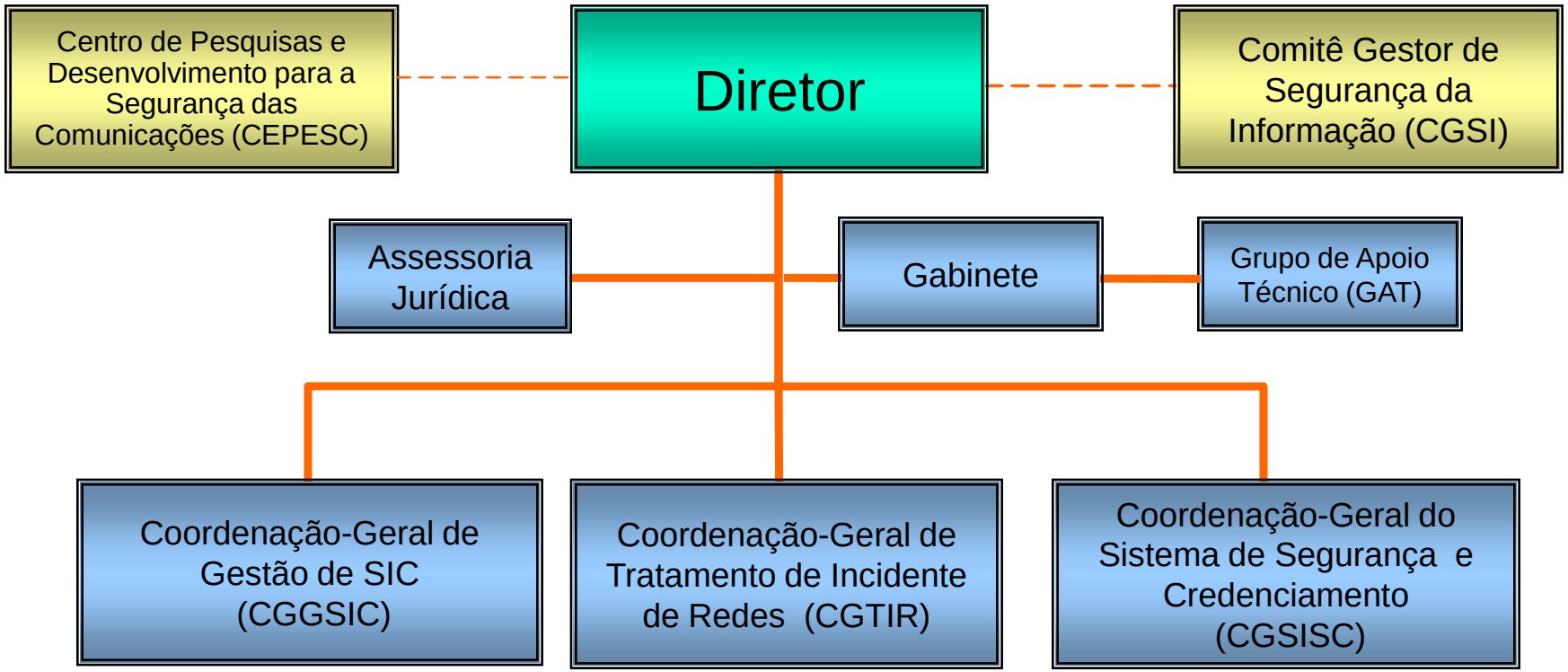
DSIC/GSI

Decreto 5772 de 08 de maio de 2006

Decreto 6931 de 11 de agosto de 2009

Planejar e Coordenar a execução das atividades de Segurança da Informação e Comunicações na Administração Pública Federal.

ORGANOGRAMA - DSIC



GESTÃO DE INCIDENTES NA APF

- Fim de 2004 a 2006
  - CTIR Gov cumpriu missão sem amparo documental

- **Missão CGTIR** (Art. 39, da Port. 13, de 04Ago2006/GSI)
  - Operar e manter o CTIR Gov
  - Promover intercâmbio
  - Apoiar órgãos e entidades da APF
  - Monitorar e analisar os incidentes da APF
  - Implementar mecanismos de avaliação de danos
  - Apoiar, incentivar e contribuir para a capacitação

AGENDA

- **APF**
- **CGTIR - CTIR Gov**
- **Ações em andamento**
- **Aspectos Jurídicos**

RELACIONAMENTOS

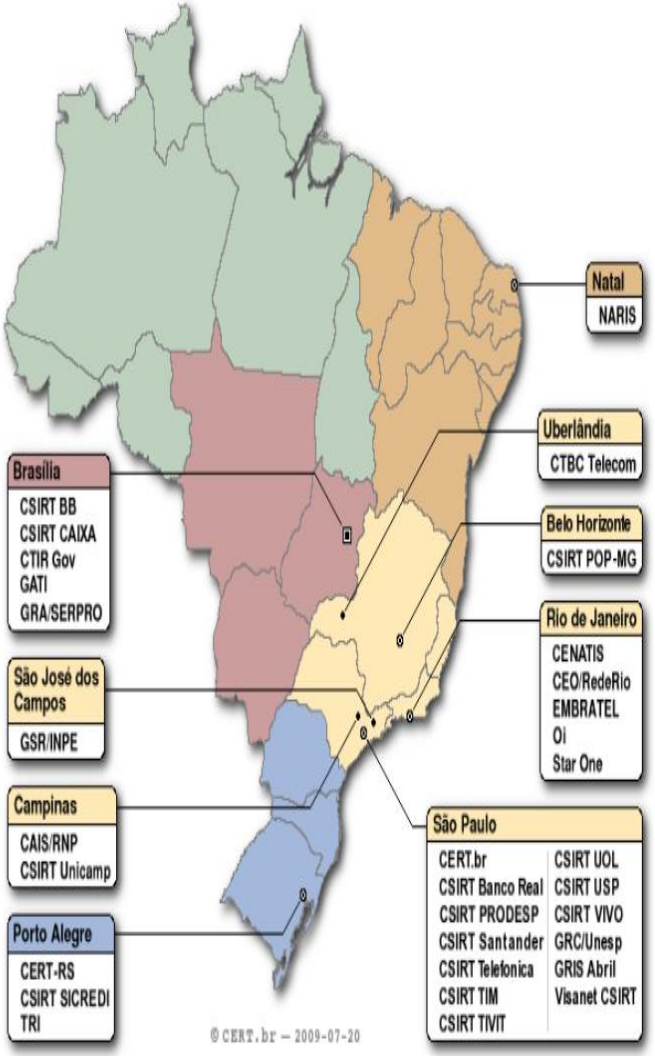
Organization of American States

Visibilidade internacional do CTIR Gov

Centros de resposta com Representação Nacional

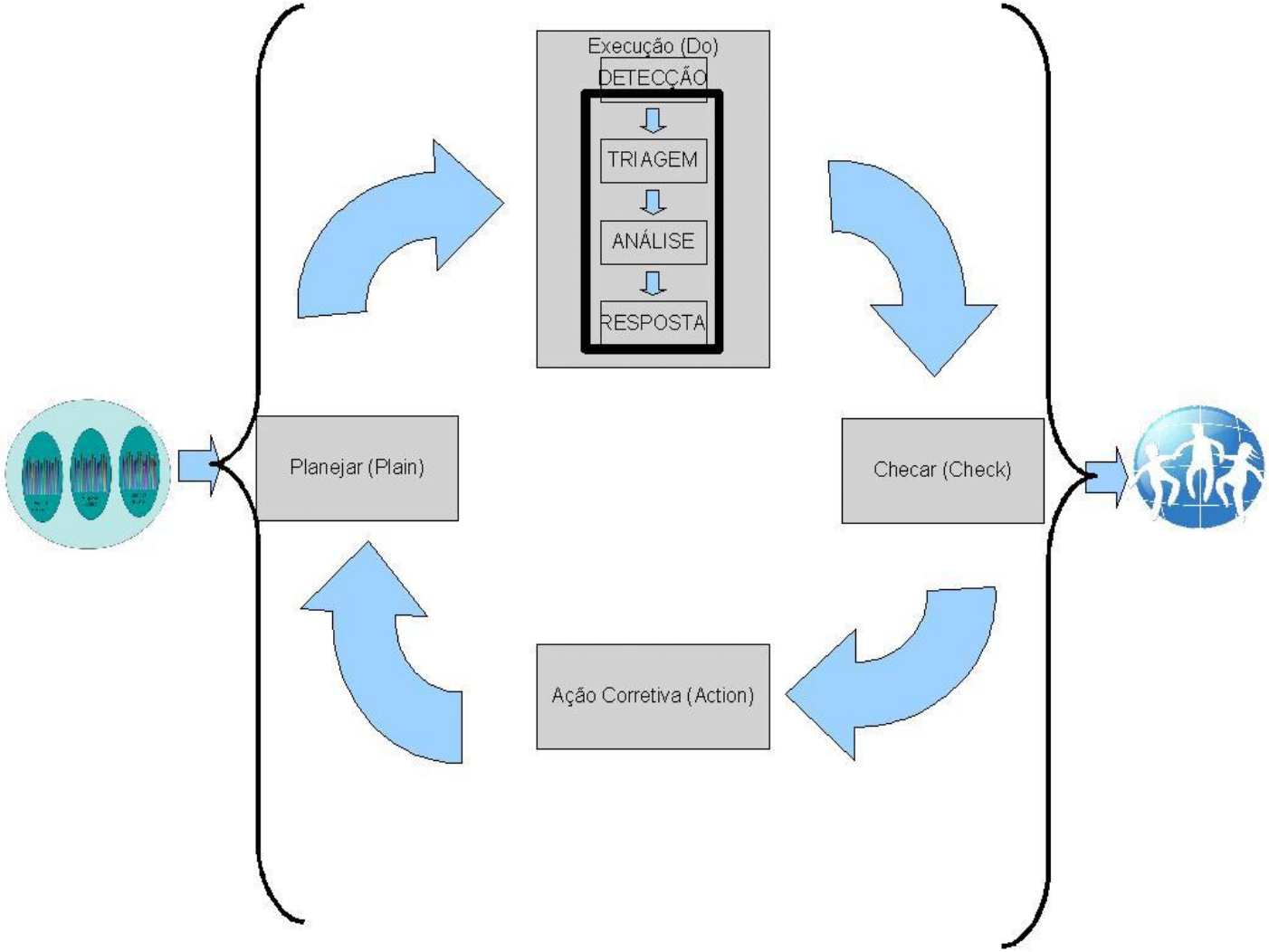
Fonte: http://www.cert.org/cert/map_open.html

Setor	CSIRTs
Resposabilidade Nacional	CERT.br **CTIR Gov**
Redes de Governo	CTIR Gov, GATI, GRA/SERPRO, CSIRT Prodesp
Setor Financeiro	CSIRT BB, CSIRT CAIXA, CSIRT Banco Real, CSIRT Sicredi, CSIRT Santander, Visanet CSIRT
Telecom/ISP	CTBC Telecom, EMBRATEL, StarOne, Oi, CSIRT Telefonica, CSIRT TIM, CSIRT UOL, CSIRT VIVO
Redes Acadêmicas e de Pesquisa	GSR/INPE, CAIS/RNP, CSIRT Unicamp, CERT-RS, NARIS, CSIRT POP-MG, CENATIS, CEO/RedeRio, CSIRT USP, GRC/UNESP, TRI
Outros	CSIRT TIVIT, GRIS Abril



GESTÃO DE INCIDENTES

Coordenação-Geral de Tratamento de Incidentes em Redes



TIPO DE TRABALHO

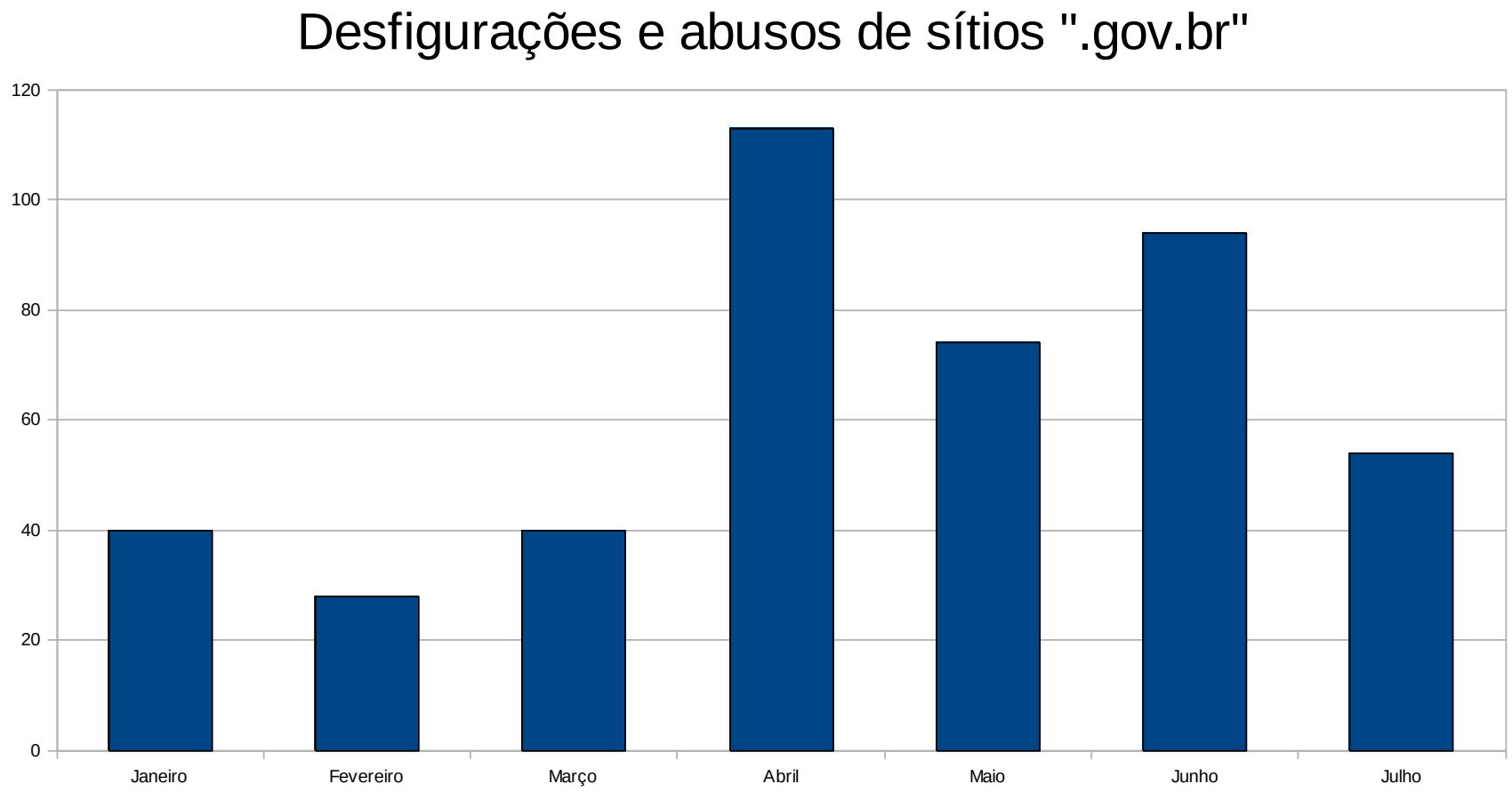
- Automático
  - Notificação de vírus-*trojans*-*worms*
  - Notificação de IDS (filtradas)

- Semi-Automático
  - Notificação de sítios desfigurados/abusados

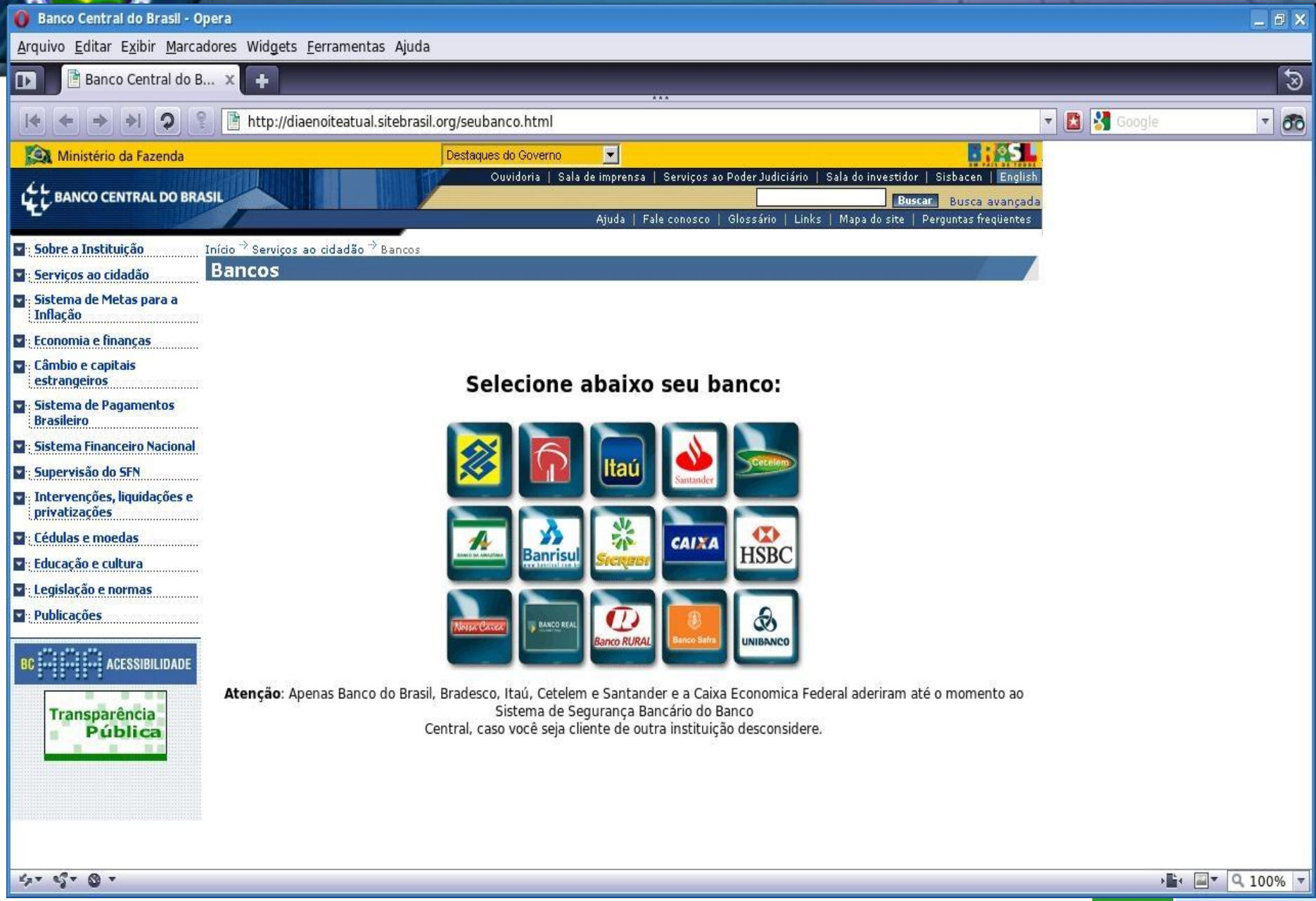
- Manual
  - Notificação de *phishing* que “chegou no destino”
  - Outros incidentes, consultas etc

ESTATÍSTICAS

Notificações enviadas (recebidas de robôs do CTIR Gov):



PHISHING - APF



PHISHING - APF

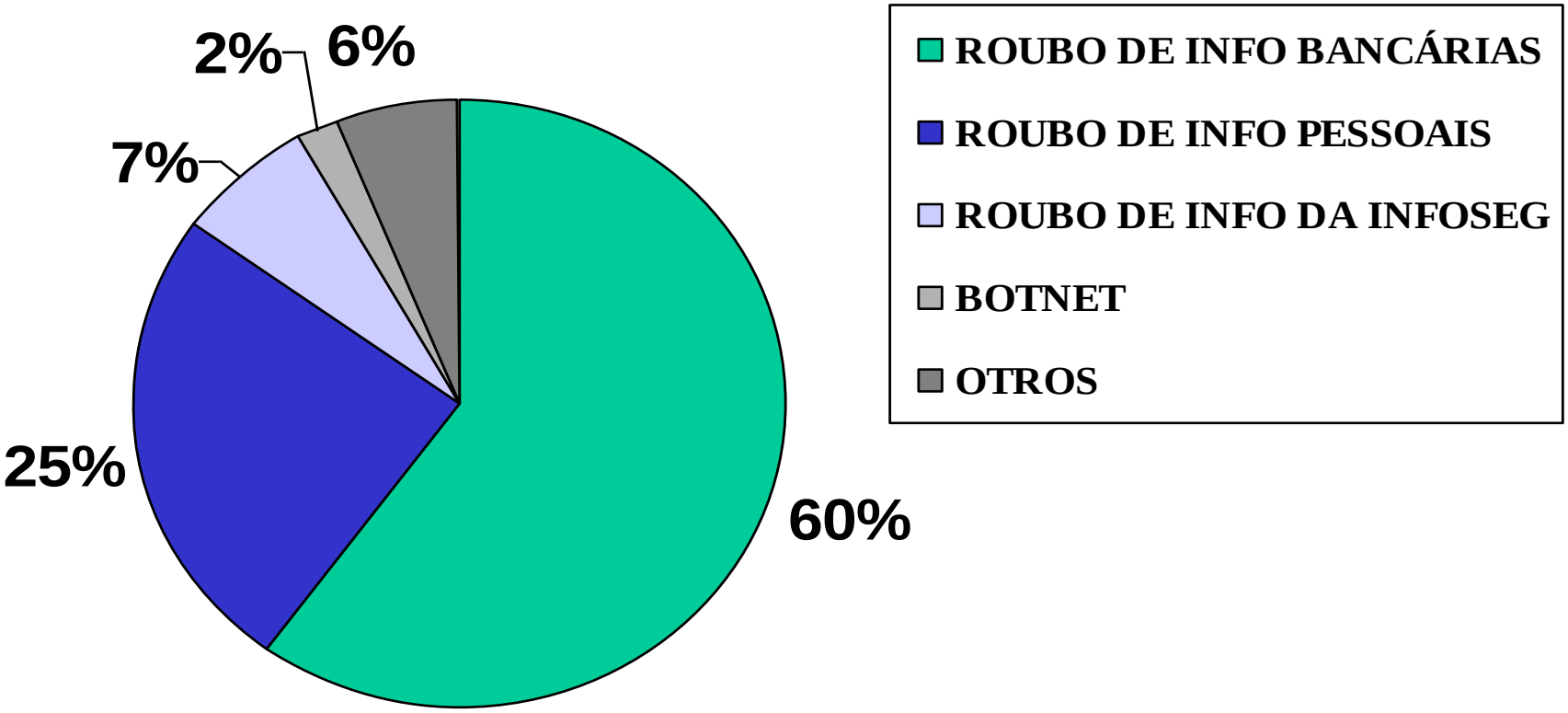
GRIPE SUINA CHEGA AO BRASIL

O **Brasil** vai receber na semana que vem 54 mil cápsulas importadas de Tamiflu, remédio recomendado pela Organização Mundial da Saúde (OMS) para o tratamento de pessoas infectadas pela gripe suína. O Ministério da Saúde divulgou nota em que informa que monitora 931 pessoas que viajaram para áreas afetadas pela doença e que apresentaram algum sintoma da doença.

Veja a seguir o video divulgado pelo **Ministério da Saúde** com as formas de prevenção e como identificar seus sintomas:

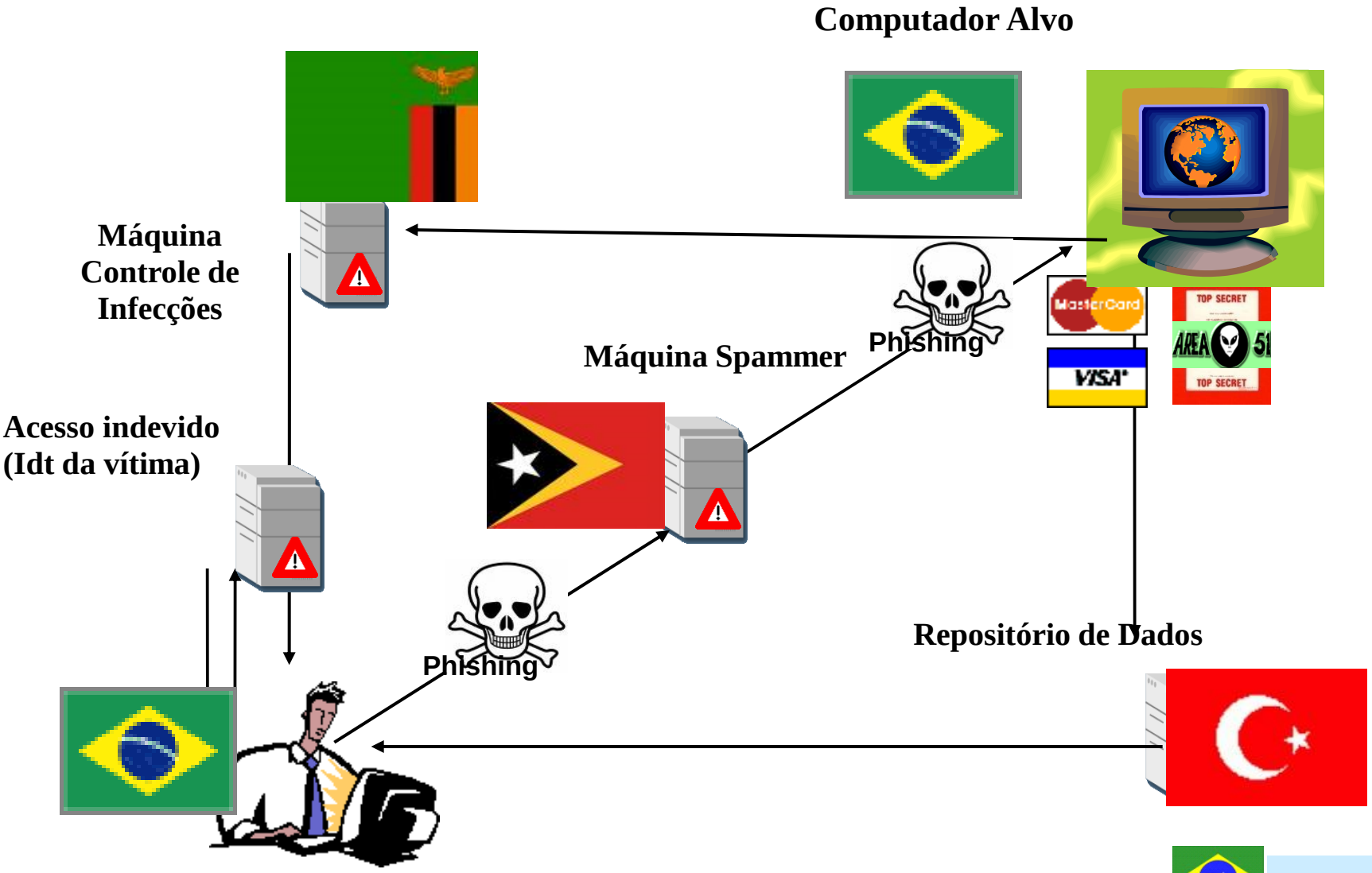
Gripe Suina - Pandemia.wav

OBJETIVOS DOS “MALWARES” na APF



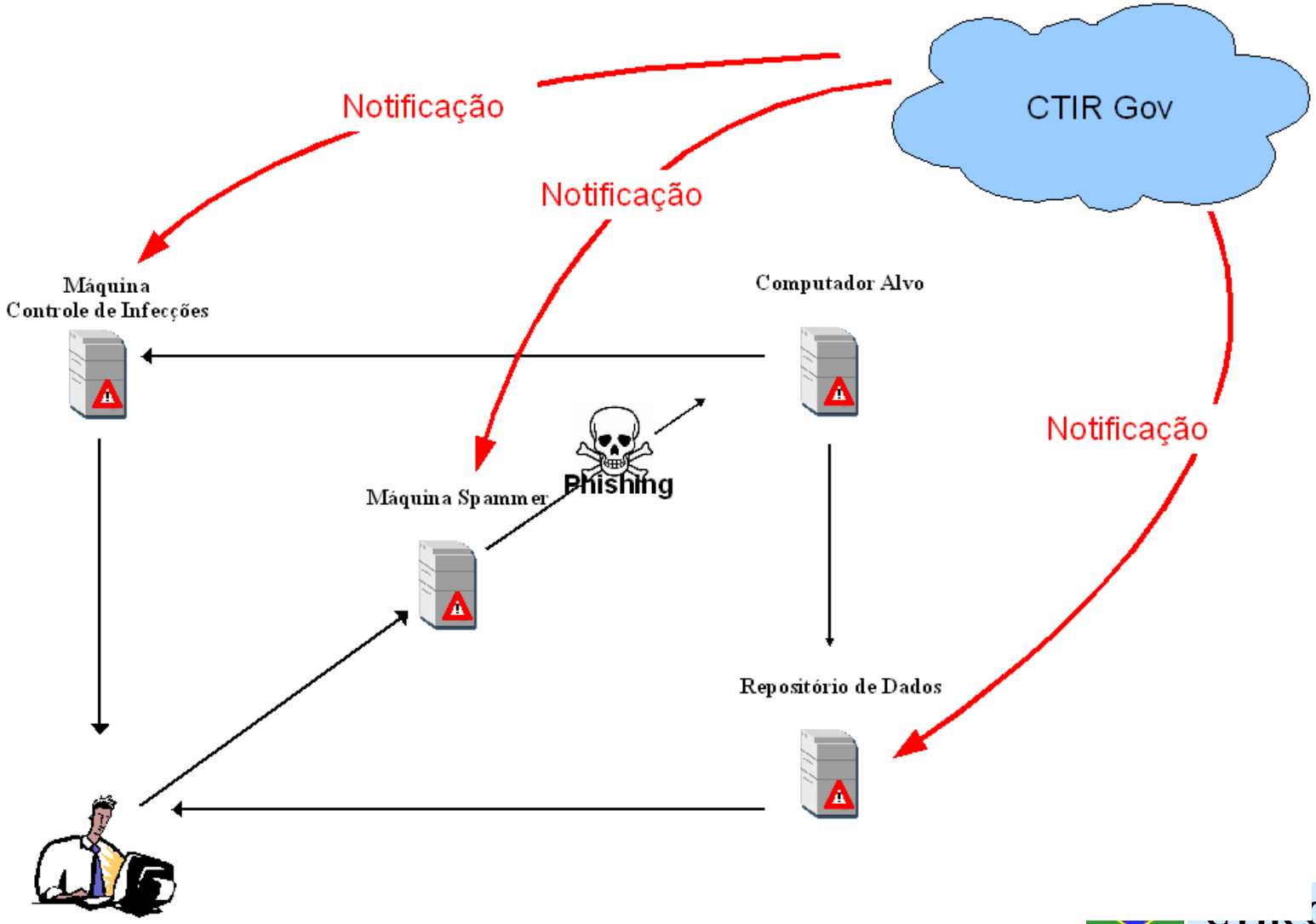
Fonte: CTIR Gov 2009

PROCESSAMENTO DE ATAQUE TÍPICO

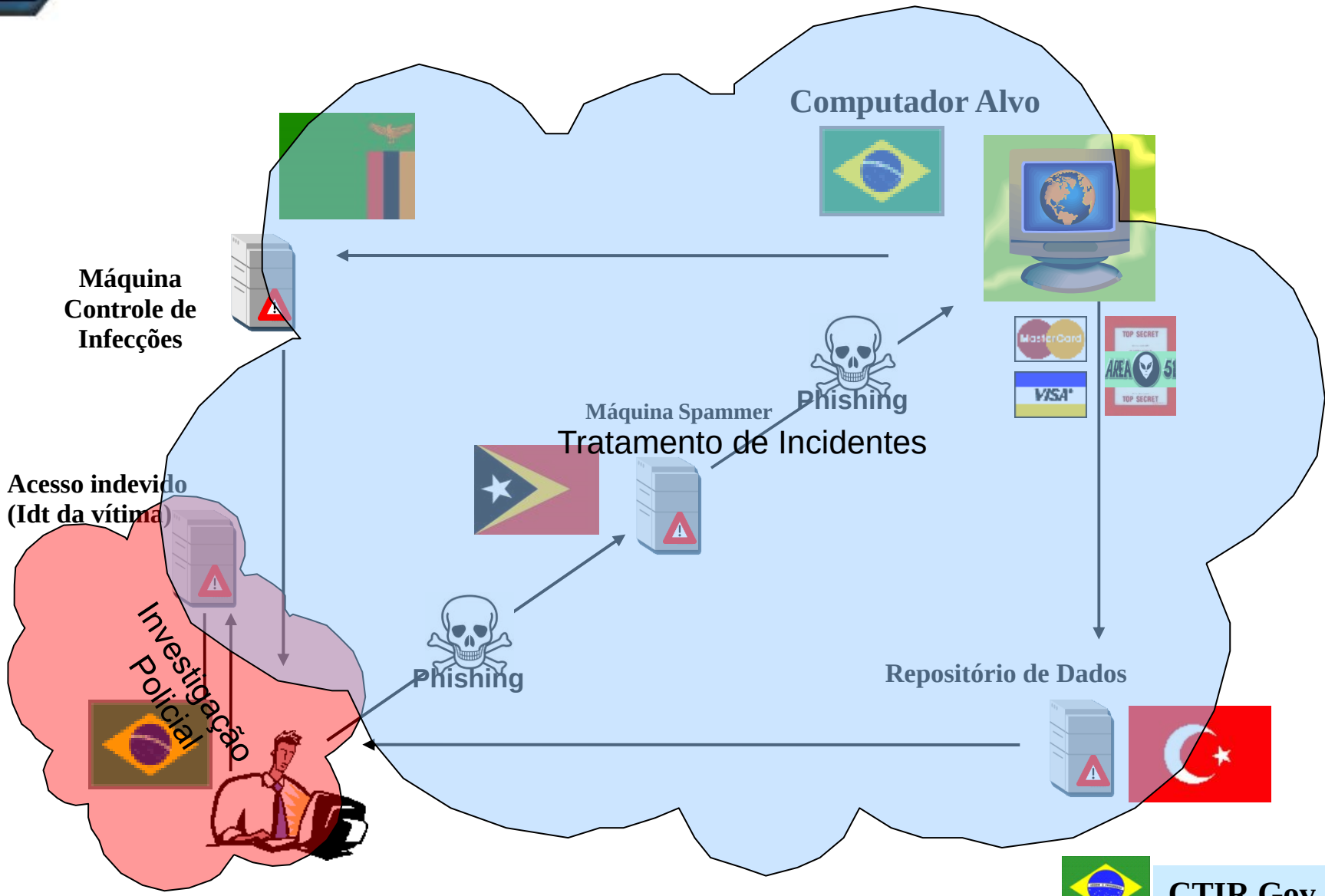


TIPO DE TRABALHO

Exemplos de notificações



TIPO DE TRABALHO



RESULTADOS DA GESTÃO DE TRATAMENTO DE INCIDENTES

- ✓ Resposta adequada aos incidentes de segurança (serviços reativos);
- ✓ Redução de riscos e impactos (serviços pró-ativos);
- ✓ Formação de uma base de conhecimento e uma referência de fácil acesso;
- ✓ Formação de uma Rede de Colaboradores;
- ✓ Formação de conhecimento sobre riscos e vulnerabilidades;
- ✓ Acompanhamento de iniciativas nacionais e internacionais na área da segurança e no tratamento de incidentes;

AGENDA

- **APF**
- **CGTIR - CTIR Gov**
- **Ações em andamento**
- **Aspectos Jurídicos**

ACÓRDÃO Nº. 1603 – 15/08/08 – TCU

- ✓48% não possui procedimentos de controle de acesso
- ✓64% não tem política de segurança da informação
- ✓64% não tem área específica de segurança da informação
- ✓75% não adota análise de riscos
- ✓76% não tem gestão de incidentes
- ✓80% não classifica as informações
- ✓84% não utiliza gestão de capacidade
- ✓88% não usa gestão de mudanças
- ✓88% não tem plano de continuidade de negócio

ACÓRDÃO Nº 2471 – 05/11/08 TCU

- Recomendar ao Gabinete de Segurança Institucional da Presidência da República que:
  - Crie procedimentos para elaboração de Políticas de Segurança da Informação, Políticas de Controle de Acesso, Políticas de Cópias de Segurança, Análises de Riscos e Planos de Continuidade do Negócio; e
  - Identifique boas práticas relacionadas à segurança da informação, difundindo-as na Administração Pública Federal.

CULTURA DE SIC NA APF

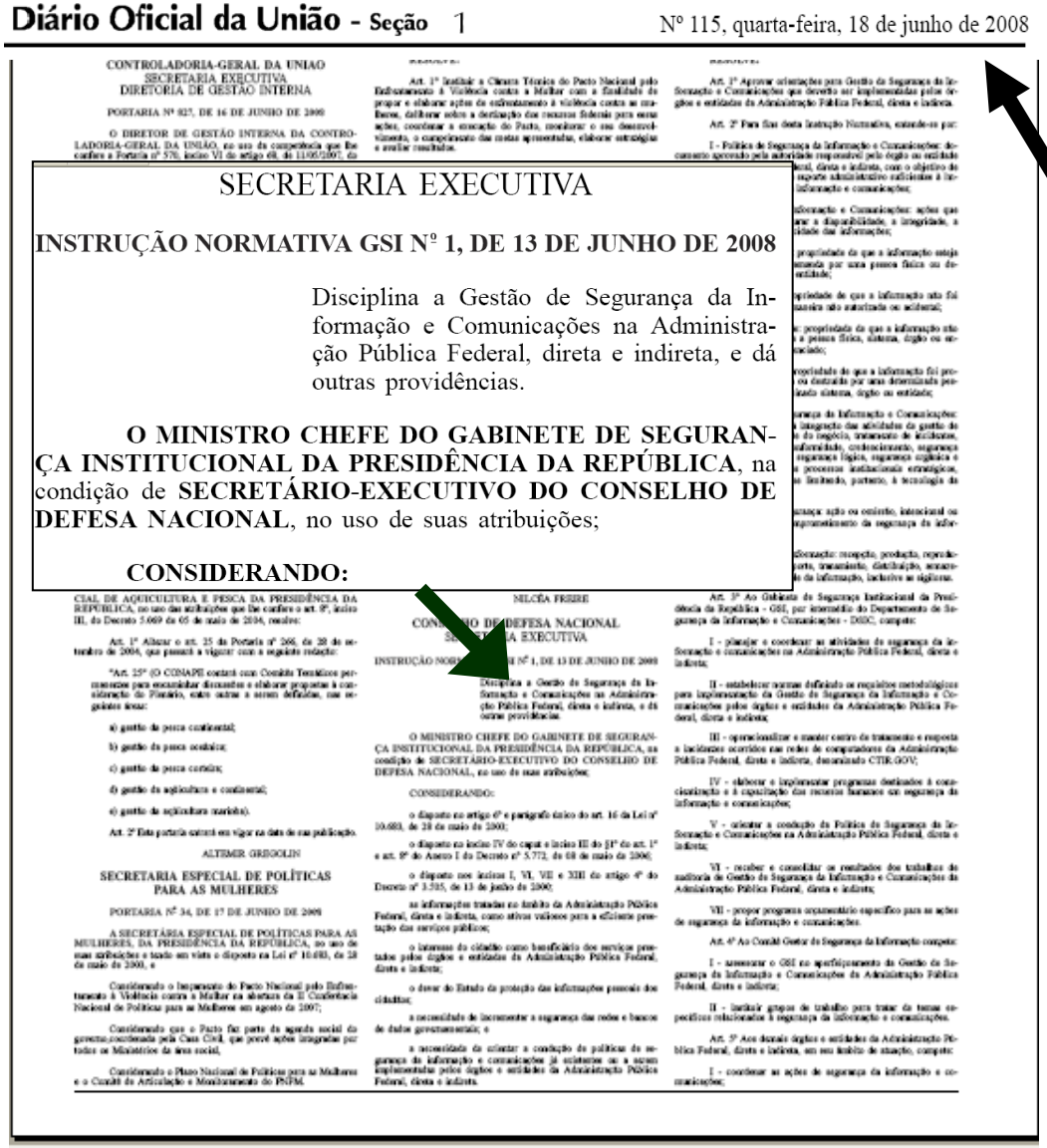
ATIVIDADE	METODOLOGIA	ALVO	REALIZADO
Sensibilização	Palestras e Congressos	1.000.000	25.517
Conscientização	Seminários e Oficinas	100.000	4.363
Capacitação	Cursos de Fundamentos	10.000	595 150
Especialização	Cursos pós-graduação	1000	80 193

NORMATIVAS DE GESTÃO DE SIC-APF

Normas de SIC aprovadas e publicadas:

- **IN GSI 01, de 13 de junho de 2008 – Gestão SIC APF**
  - **NC 01, de 14 de outubro de 2008 – Normalização**
  - **NC 02, de 15 de outubro de 2008 – Metodologia**
  - **NC 03, de 03 de julho de 2009 – POSIC**
  - **NC 04, de 17 de agosto de 2009 - GRSIC**
  - **NC 05, de 17 de agosto de 2009 – ETIR**
  - **NC 06, de 11 de novembro de 2009 – GCN**
  - **NC 07, de 14 de abril de 2010 – CASIC**
  - **NC 08, de 24 de agosto de 2010 – Gestão de ETIR**
- **Normas em estudo: Manual do Gestor de SIC (2010); e Uso de criptografia na APF (2010).**

INSTRUÇÃO NORMATIVA Nº 01



Diário Oficial da União - Seção 1 Nº 115, quarta-feira, 18 de junho de 2008

SECRETARIA EXECUTIVA

INSTRUÇÃO NORMATIVA GSI Nº 1, DE 13 DE JUNHO DE 2008

Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.

O MINISTRO CHEFE DO GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA, na condição de **SECRETÁRIO-EXECUTIVO DO CONSELHO DE DEFESA NACIONAL**, no uso de suas atribuições;

CONSIDERANDO:

INSTRUÇÃO NORMATIVA Nº 01

Art. 3º Atribuições do GSI

Ao Gabinete de Segurança Institucional da Presidência da República – GSIPR, por intermédio do Departamento de Segurança da Informação e Comunicações – DSIC, compete:

I - planejar e coordenar as atividades de segurança da informação e comunicações na Administração Pública Federal, direta e indireta;

II - estabelecer normas definindo os requisitos metodológicos para implementação da Gestão de Segurança da Informação e Comunicações pelos órgãos e entidades da Administração Pública Federal, direta e indireta;

III - operacionalizar e manter centro de tratamento e resposta a incidentes ocorridos nas redes de computadores da Administração Pública Federal, direta e indireta, denominado CTIR.GOV;

IV - elaborar e implementar programas destinados à conscientização e à capacitação dos recursos humanos em segurança da informação e comunicações;

V - orientar a condução da Política de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta;

VI - receber e consolidar os resultados dos trabalhos de auditoria de Gestão de Segurança da Informação e Comunicações da Administração Pública Federal, direta e indireta;

VII - propor programa orçamentário específico para as ações de segurança da informação e comunicações.

INSTRUÇÃO NORMATIVA Nº 01

Art. 3º Atribuições do GSI

Ao Gabinete de Segurança Institucional da Presidência da República – GSIPR, por intermédio do Departamento de Segurança da Informação e Comunicações – DSIC, compete:

I - planejar e coordenar as atividades de segurança da informação e comunicações na Administração Pública Federal, direta e indireta;

II - estabelecer normas definindo os requisitos metodológicos para implementação da Gestão de Segurança da Informação e Comunicações pelos órgãos e entidades da Administração Pública Federal, direta e indireta;

III - operacionalizar e manter centro de tratamento e resposta a incidentes ocorridos nas redes de computadores da Administração Pública Federal, direta e indireta, denominado CTIR.GOV;

IV - elaborar e implementar programas destinados à conscientização e à capacitação dos recursos humanos em segurança da informação e comunicações;

V - orientar a condução da Política de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta;

VI - receber e consolidar os resultados dos trabalhos de auditoria de Gestão de Segurança da Informação e Comunicações da Administração Pública Federal, direta e indireta;

VII - propor programa orçamentário específico para as ações de segurança da informação e comunicações.

Art. 5º Atribuições dos demais órgãos

Aos demais órgãos e entidades da Administração Pública Federal, direta e indireta, em seu âmbito de atuação, compete:

I - coordenar as ações de segurança da informação e comunicações;

II - aplicar as ações corretivas e disciplinares cabíveis nos casos de quebra de segurança;

III - propor programa orçamentário específico para as ações de segurança da informação e comunicações;

IV - nomear Gestor de Segurança da Informação e Comunicações;

V - instituir e implementar equipe de tratamento e resposta a incidentes em redes computacionais;

VI - instituir Comitê de Segurança da Informação e Comunicações;

VII - aprovar Política de Segurança da Informação e Comunicações e demais normas de segurança da informação e comunicações;

VIII - remeter os resultados consolidados dos trabalhos de auditoria de Gestão de Segurança da Informação e Comunicações para o GSIPR.

Art. 7º Atribuições do Gestor de SIC

Ao Gestor de Segurança da Informação e Comunicações, no âmbito de suas atribuições, incumbe:

I - promover cultura de segurança da informação e comunicações;

II - acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

III - propor recursos necessários às ações de segurança da informação e comunicações;

IV - coordenar o Comitê de Segurança da Informação e Comunicações e a equipe de tratamento e resposta a incidentes em redes computacionais;

V - realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;

VI - manter contato direto com o DSIC para o trato de assuntos relativos à segurança da informação e comunicações;

VII - propor normas relativas à segurança da informação e comunicações.

Art. 8º O cidadão, como principal cliente da Gestão de Segurança da Informação e Comunicações da Administração Pública Federal, direta e indireta, poderá apresentar sugestões de melhorias ou denúncias de quebra de segurança que deverão ser averiguadas pelas autoridades.

NC nº 03 - POSIC

PORTARIA Nº 29, DE 30 DE JUNHO DE 2009

Homologa a Norma Complementar nº 03/IN01/DSIC/GSIPR.

O MINISTRO DE ESTADO CHEFE DO GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA, na condição de **SECRETÁRIO-EXECUTIVO DO CONSELHO DE DEFESA NACIONAL**, no uso da atribuição que lhe confere o Art. 4º do Decreto nº 3.505, de 13 de junho de 2000, e o inciso IV do art. 1º do Anexo I do Decreto nº 5.772, de 08 de maio de 2006, resolve:

Art. 1º Fica homologada a Norma Complementar nº 03 que estabelece diretrizes para elaboração de Política de Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal, aprovada pelo Diretor do Departamento de Segurança da Informação e Comunicações.

Art. 2º Esta portaria entra em vigor na data de sua publicação.

JORGE ARMANDO FELIX

NC nº 03 - POSIC

A **POSIC** é um documento que registra as diretrizes **estratégicas, responsabilidades, competências** e **o apoio** para implementar a gestão de SIC da APF.

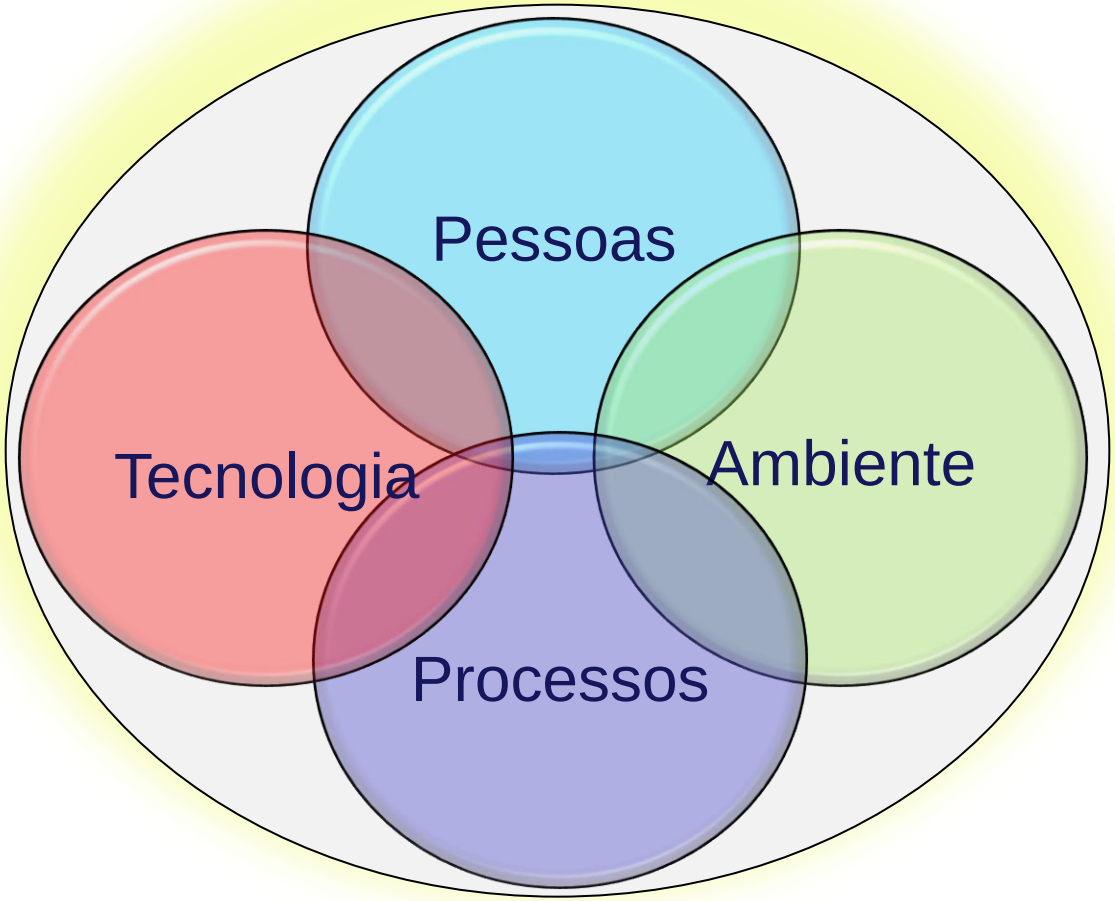
- visa viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação (DICA).

- Expressa a **importância** que a Organização dá para a **informação**.

- Declara o **comprometimento** da **alta direção** da Organização para implementar a gestão de SIC.

- Informa o que **deve ser feito** na Organização.

O que deve ser contemplado?



Ativos de Informação

NC nº 03 - POSIC

Itens recomendados

Estrutura da POSIC

- Escopo
- Conceitos e definições
- Referências legais e normativas
- Princípios
- Diretrizes Gerais
- Penalidades
- Competências e Responsabilidades
- Atualização

NC nº 05 - ETIR

PORTARIA Nº 38, DE 14 DE AGOSTO DE 2009

Homologa a Norma Complementar nº 05/IN01/DSIC/GSIPR.

O MINISTRO DE ESTADO CHEFE DO GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA, na condição de **SECRETÁRIO-EXECUTIVO DO CONSELHO DE DEFESA NACIONAL**, no uso da atribuição que lhe confere o Art. 4º do Decreto nº 3.505, de 13 de junho de 2000, e o inciso IV do art. 1º do Anexo I do Decreto nº 5.772, de 08 de maio de 2006, resolve:

Art. 1º Fica homologada a Norma Complementar nº 05/IN01/DSIC/GSIPR que disciplina a criação de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal, aprovada pelo Diretor do Departamento de Segurança da Informação e Comunicações, em anexo.

Art. 2º Esta portaria entra em vigor na data de sua publicação.

JORGE ARMANDO FELIX

NC nº 05 - ETIR

Responsabilidade

- Os **Gestores de Segurança da Informação e Comunicações** são os responsáveis por coordenar a instituição, implementação e manutenção da infra-estrutura necessária às Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais.

Definição da Missão

- A missão deve fornecer uma breve e inequívoca descrição dos objetivos básicos e a função da ETIR.

Modelo de Implementação

- Cada órgão ou entidade deverá estabelecer aquele que melhor se adequar às suas necessidades e limitações.
  - **Utilizando a equipe de Tecnologia da Informação - TI**
  - **Centralizado**
  - **Descentralizado**
  - **Combinado ou Misto**

NC nº 05 - ETIR

Estrutura Organizacional

- A estrutura dependerá do modelo de implementação a ser adotado, do tamanho da organização, do número de localizações geográficas, do número de sistemas e plataformas suportadas, do número de serviços a serem oferecidos e do conhecimento técnico do pessoal existente.

Autonomia da ETIR

- A autonomia descreve o escopo de atuação e o nível de responsabilidade que a Equipe tem sobre as suas próprias ações e sobre as atividades de resposta e tratamento dos incidentes na rede de computadores.
  - **Autonomia Completa**
  - **Autonomia Compartilhada**
  - **Sem Autonomia**

Anexo A

Documento de Constituição da ETIR

- A fim de regulamentar o funcionamento da ETIR, os órgãos e entidades da APF deverão elaborar e publicar o **Documento de Constituição da ETIR**, alinhado com a Política de Segurança da Informação e Comunicações, devidamente aprovado pela Alta Administração do órgão ou entidade.
- No documento de constituição da ETIR deverão constar, no mínimo, os seguintes pontos:
  - **Missão;**
  - **Comunidade ou público alvo;**
  - **Modelo de implementação;**
  - **Estrutura organizacional;**
  - **Autonomia da ETIR;**
  - **Serviços que serão prestados.**

MUITO OBRIGADO !

Eduardo **Wallier** Vianna

Coordenador Geral de Tratamento de Incidentes de Rede

cgtir@planalto.gov.br

http://www.ctir.gov.br

ctir@ctir.gov.br (para as Notificações)

http://dsic.planalto.gov.br - NORMAS

AGENDA

- **APF**
- **CGTIR - CTIR Gov**
- **Ações em andamento**
- **Aspectos Jurídicos**

O QUE UM ASSESSOR JURÍDICO TERIA A TRANSMITIR DIANTE DO CONTEÚDO ATÉ ENTÃO APRESENTADO?

VOCÊ JÁ DIGITOU SEU NOME NO GOOGLE HOJE?

Condenado 1ª instância e absolvido em 2ª / ação de despejo

ASPECTOS JURÍDICOS E ÉTICOS DE SIC

YouTube é multado por manter vídeo considerado ofensivo por Netinho

Empresa deverá pagar multa de R$ 30 mil.
Companhia ainda pode recorrer da decisão.

Google ainda pode recorrer de decisão favorável ao cantor Netinho.

A Justiça Eleitoral multou em R$ 30 mil o Google Brasil por não ter retirado do YouTube um vídeo considerado ofensivo pelo cantor e candidato do PC do B derrotado nas eleições para o Senado em São Paulo, Netinho de Paula.

O valor da ação movida por Netinho e pela coligação União para Mudar, formada pelos partidos PRB, PDT, PT, PTN, PR, PSDC, PRTB, PRP, PC do B e PT do B, exige que a empresa pague uma multa no valor de R$ 30 mil. Além da multa, a empresa terá que pagar R$ 10 mil diários, do dia 1º de outubro até a eleição, pelo descumprimento da liminar que exigia a retirada do vídeo.

De acordo com a sentença publicada no site do Tribunal Regional Eleitoral de São Paulo, o juiz auxiliar da propaganda eleitoral Mário Devienne Ferraz considerou que o vídeo tem “conteúdo ofensivo, porque atribui ao candidato representante [Netinho] a prática de agressões físicas contra mulher e repórter humorístico”.

Ele considerou que o Google é responsável pelo "conteúdo prejudicial do site que hospeda, ainda que seja apenas provedor de hospedagem". Segundo o juiz, o Google deveria retirar o vídeo do YouTube "quando tiver ciência comprovada do ilícito". O Google ainda pode recorrer da decisão.

Procurado pelo G1, o Google, por meio de sua assessoria de imprensa, afirmou não ter conhecimento da multa e que "estudaria o caso". O G1 também entrou em contato com a assessoria de imprensa do candidato, mas não deu mais detalhes sobre o processo até o momento.

Fonte: http://g1.globo.com/tecnologia/noticia/2010/10/youtube-e-multado-por-manter-no-ar-video-considerado-ofensivo-por-netinho.html

ASPECTOS JURÍDICOS E ÉTICOS DE SIC

Receita regulamenta medidas para disciplinar acesso a dados sigilosos Publicidade

A Receita Federal publicou na edição desta quarta-feira do "Diário Oficial da União" portaria para disciplinar o acesso a informações fiscais sigilosas. De acordo com o texto, são autorizados a acessarem esses dados servidores que possuam permissão de acesso ou que pertençam aos quadros da Receita ou estejam prestando serviços para o órgão ...(vazamento de informações da receita). A norma aponta que são protegidas por sigilo informações como: as atividades relativas a rendas, patrimônio, débitos, créditos, dívidas e movimentação financeira e patrimonial; aquelas que revelem negócios, contratos e relacionamentos comerciais; as relativas a processos industriais. Essas informações só poderão ser acessadas por necessidade de ofício do servidor autorizado. A portaria também discrimina quais dados não são protegidos por sigilo, como informações cadastrais, por exemplo. No texto, a Receita informa que atitudes como acesso a bancos de dados sem permissão, assim como acessos sem justificativa, são considerados indevidos e passíveis de punição que vão desde suspensão a até demissão. A atribuição de autorização para acesso aos dados sigilosos será realizada quando a ação for necessária para fins de fiscalização, acompanhamento, investigação e outras medidas, respeitada a função do servidor. A portaria ainda regulamenta a emissão de procurações que o contribuinte poderá realizar para que terceiros tenham acesso aos seus dados. As procurações só poderão ser feitas mediante sistema de certificação eletrônica obtida em cartório. **O texto ainda institui o Comitê de Segurança da Informação Protegida por Sigilo Fiscal**, responsável por dirimir controvérsias e esclarecer dúvidas sobre classificação, grau de sigilo fiscal e de informações sob a guarda da Receita Federal. Esse órgão será composto de representante das subsecretarias, da Coordenação-Geral de Pesquisa e Investigação e da Coordenação-Geral de Auditoria Interna.

Fonte: http://www1.folha.uol.com.br/poder/813847-receita-regulamenta-medidas-para-disciplinar-acesso-a-dados-sigilosos.shtml

ASPECTOS JURÍDICOS E ÉTICOS DE SIC

Segurança da Informação: proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, 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 (Decreto nº 3.505, 13 de junho de 2000)

Segurança da Informação e Comunicações: ações que objetivam viabilizar e assegurar a disponibilidade (acessível e utilizável), a integridade (sem modificação ou destruição não autorizada ou acidental) , a confidencialidade (disponível somente para autorizados)e a autenticidade (produzida, expedida, modificada ou destruída por determinada pessoa física, ou sistema, órgão ou entidade) das informações (Instrução Normativa nº 01/GSI, 13 de junho de 2000)

Quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações (Instrução Normativa nº 01/GSI, 13 de junho de 2000)

A RESPOSTA ESTÁ NO FATO DE QUE OS CONCEITOS CITADOS REVELAM QUE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES NÃO SE RESTRINGE A TI E ESTÁ INTIMAMENTE RELACIONADO AO COMPORTAMENTO , POR VIA DE CONSEQUÊNCIA, DEVE-SE FALAR EM MUDANÇA DE COMPORTAMENTO.

POTENCIAL LESIVO DA INTERNET

“VERBA VOLANT SCRIPTA MANENT”

MAS DE QUE MUDANÇA ESTOU FALANDO?

EX. DIGA-ME COM QUEM ANDAS E TE DIREI QUEM ÉS / DIGA-ME COM QUEM TECLAS OU COM QUEM SE RELACIONA NAS COMUNIDADES VIRTUAIS...

EX. NÃO CONVERSE COM PESSOAS ESTRANHAS / MAS VOCÊ SABE COM QUEM ESTÁ TECLANDO? OU COM QUEM SEU FILHO ESTÁ TECLANDO??????

EX. NÃO PEGUE O QUE NÃO É SEU / CTRL C e CTRL V NO CONTEÚDO ALHEIO

EX. SUA SENHA É PESSOAL E INTRANSFERÍVEL? AONDE ELA ESTÁ ANOTADA? SUA SECRETÁRIA A CONHECE? SUA ESPOSA A CONHECE?

EX. DEIXAR O FERRO LIGADO OU A PORTA ABERTA AO SAIR DE CASA / E O COMPUTADOR LOGADO, COMO DEVO PROCEDER?

EX. JAMAIS ASSINE QUALQUER DOCUMENTO SEM LER O QUE ESTÁ ESCRITO / VC LEU O CONTRATO DE COMPRA DE SUA PASSAGEM AÉREA?

EX. VOCÊ LEU O CONTRATO DA CONTA GRATUITA DE E-MAIL?

- **dados podem ser usados após encerramento da conta;**
- **Não se garante a segurança da informação em e-mail particular;**
- **Serviço pode ser cancelado sem aviso prévio e sem back up.**

EX. CIDADE PEQUENA – MENINA ENGRAVIDA – MUDANÇA DA CIDADE / FILME OU FOTO NA INTERNET (PRIVACIDADE) SEM AUTORIZAÇÃO – MUDO DE PLANETA?

ASPECTOS JURÍDICOS E ÉTICOS DE SIC

MAS DE QUE MUDANÇA ESTOU FALANDO?

EX. FALAR MAL DO CHEFE NO CAFEZINHO / COMUNIDADE “MEU CHEFE É UM ...”

EX. DESABAFOS OU PROMESSAS CONJUGAIS FALADOS NÃO SÃO MEIOS DE PROVA SENÃO PROVADOS / E SE FOREM POSTADOS? ELES ESTÃO NA MÁQUINA.

EX. NÃO ABRA A PORTA PARA ESTRANHOS / NÃO ABRA O E-MAIL DE ESTRANHOS

EX. SEQUESTRO RELÂMPAGO – COMUNIDADE DO FILHO: “QUEM TEM O PAI MAIS RICO”.

EX. OS FINS NÃO JUSTIFICAM OS E-MAILS – DISCUTIR VULNERABILIDADES ENTRE FUNCIONÁRIOS EM REDE PODE EXPOR UM ÓRGÃO, AINDA QUE A INTENÇÃO SEJA A DE RESOLVER UM PROBLEMA.

EX. QUEM TEM UM CELULAR? ELE TEM SENHA? COMO PROTEGER OS DADOS NELE CONTIDOS?

EX. SEU CELULAR TIRA FOTOS? E O DIREITO DE IMAGEM?

EX. VOCÊ TEM UM SMARTPHONE? JÁ INSTALOU ANTIVÍRUS?

EX. DIREITOS AUTORAIS – O CONTEÚDO DA MINHA PALESTRA PODE SER GRAVADO SEM AUTORIZAÇÃO? É PARA USO PRÓPRIO? POSSO DISPONIBILIZAR O CONTEÚDO NA INTERNET?

EX. DANIELA CICARRELI – PORQUÊ O CONTEÚDO POSTADO NA INTERNET FOI RETIRADO DO AR SE O LUGAR ONDE FOI GRAVADO ERA PÚBLICO? FOI EDITADO E OBJETIVOU LUCRO.

QUEM É O DESTINATÁRIO DESSA MUDANÇA?

Servidor público é todo aquele que, por força de lei, contrato ou de qualquer ato jurídico, preste serviços de natureza permanente, temporária ou excepcional, ainda que sem retribuição financeira, desde que ligado direta ou indiretamente a qualquer órgão do poder estatal, como as autarquias, as fundações públicas, as entidades paraestatais, as empresas públicas e as sociedades de economia mista, ou em qualquer setor onde prevaleça o interesse do Estado. (Código de Ética do Servidor Público)

Art. 327 (CP) - Considera-se funcionário público, para os efeitos penais, quem, embora transitoriamente ou sem remuneração, exerce cargo, emprego ou função pública.

§ 1º - Equipara-se a funcionário público quem exerce cargo, emprego ou função em entidade paraestatal, e quem trabalha para empresa prestadora de serviço contratada ou conveniada para a execução de atividade típica da Administração Pública179.

§ 2º - A pena será aumentada da terça parte quando os autores dos crimes previstos neste Capítulo forem ocupantes de cargos em comissão ou de função de direção ou assessoramento de órgão da administração direta, sociedade de economia mista, empresa pública ou fundação instituída pelo poder público

QUEBRA DE SEGURANÇA QUE COMPROMETA A DICA IMPLICA EM RESPONSABILIDADE:

- **ADMINISTRATIVA**
- **CIVIL**
- **PENAL**

CRIMES DIGITAIS OU CIBERNÉTICOS

Ou Cybercrime consiste toda conduta criminosa em que o processamento eletrônico de dados serve como meio para a prática do delito ou é alvo desse ato

- **IMPRÓPRIOS – conduta ilícita praticada através de um sistema informatizado (previstos no Código Penal – 95%). O processamento eletrônico é o meio para cometimento do delito.**

- **PRÓPRIOS – só podem ser cometidos em meios eletrônicos.**

IMPRÓPRIOS

Daqueles 95%, 70% das condutas são punidas eficientemente e o restante é punido, mas com alguma deficiência.

Ex. disseminar código malicioso e como consequência derruba-se uma rede. Tipo não específico. Dano (pena inferior a um ano) - PL

- crimes contra a honra: calúnia (art. 138, CP); difamação (art. 139, CP); injúria (art. 140, CP);

- fraudes bancárias e de cartão de crédito;

- pornografia infantil;

- falsificação e adulteração de dados e documentos a exemplo de cheques e cartões de crédito.

CTRL C / CTRL V

CP, art. 153 § 1º: detenção de 1 a 4 anos e multa por crime de divulgação de informação sigilosa contida ou não nos sistemas ou bancos de dados da Administração Pública.

CP, art. 154: detenção de 3 meses a 1 ano ou multa - violação de segredo profissional.

CP, art. 184: detenção de 3 meses a 1 ano - Violação de Direito Autoral;

Art. 195 da Lei 9.279/96 (Concorrência desleal).

É crime de furto (um a quatro anos de RECLUSÃO)?

Qual o momento da consumação?

E CTRL X?

PRÓPRIOS (Substitutivo 89/03 ao PL 84/99)

1) Criar e propagar phishing – forma de captação de dados de usuário – estelionato eletrônico (art. 171);
2) Falsificar ou alterar dado eletrônico ou documento público (art. 297);
3) Falsificar ou alterar dado eletrônico ou documento particular – cartão de crédito (art. 298);
4) Dano – destruir, inutilizar ou deteriorar coisa alheia ou dado eletrônico alheio – pichar um site (art. 163)

PRÓPRIOS (Substitutivo 89/03 ao PL 84/99)

5) Inserir ou difundir código malicioso – criar ou propagar vírus (art. 163-A);

6) Inserir ou difundir código malicioso seguido de dano – vírus derruba uma rede (art. 163-A);

7) Acessar redes ou sistemas expressamente protegidos sem autorização – invasões a sistemas (art. 285-A);

8) Obter ou transferir informações disponíveis em redes ou sistemas sem autorização – invasão do sistema com apropriação de dados (art. 285-B);

PRÓPRIOS (Substitutivo 89/03 ao PL 84/99)

9) Divulgar ou usar indevidamente dados e informações pessoais – ter acesso autorizado a dados e informações e utilizá-los de forma inadequada ou pública sem autorização (art. 154-A)

10) Atentado contra a segurança de serviço de utilidade pública – água, luz, calor, informação, telecomunicação etc. (art. 265);

11) Interrupção ou perturbação de serviço telegráfico, informático, telemático, dispositivo de comunicação, rede de computadores ou sistema informatizado (art. 266);

PRÓPRIOS (Substitutivo 89/03 ao PL 84/99)

12) Os provedores de acesso a internet deverão armazenar por três anos os dados de origem, data, hora e local dos acessos feitos por intermédio de suas redes.

ASPECTOS JURÍDICOS E ÉTICOS DE SIC

Lei nº 11.829/08 – altera o ECA

Art. 241-B. Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:

Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.

§ 2º Não há crime se a posse ou o armazenamento tem a finalidade de comunicar às autoridades competentes a ocorrência das condutas descritas nos arts. 240, 241, 241-A e 241-C desta Lei, quando a comunicação for feita por:

I – agente público no exercício de suas funções;

§ 3º As pessoas referidas no § 2º deste artigo deverão manter sob sigilo o material ilícito referido.

CRIMES FUNCIONAIS:

CP, art. 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano (Pena – reclusão, de 2 a 12 anos, e multa) - Vítima: Estado e o cidadão.

CP, art. 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente (Pena – detenção, de 3 (três) meses a 2 (dois) anos, e multa)

Parágrafo único. As penas são aumentadas de um terço até a metade se da modificação ou alteração resulta dano para a Administração Pública ou para o administrado.

CP, art. 314 - Extraviar livro oficial ou qualquer documento, de que tem a guarda em razão do cargo; sonegá-lo ou inutilizá-lo, total ou parcialmente (Pena - reclusão, de um a quatro anos, se o fato não constitui crime mais grave)

Crimes mais comuns cometidos no ciberspace

1) Montar página com anúncios de serviços de prostituição (Favorecimento da prostituição - Art. 228 do C.P.)

2) Criar uma comunidade ou montar homepage incitando o uso de entorpecentes ou qualquer outro crime (Apologia de crime ou fato criminoso - Art. 287 do C.P.)

3) Usar certificado digital de terceiro (Falsa identidade - Art. 307 do C.P.)

4) Entrar no sistema da Fazenda e transferir dinheiro de precatório (Exercício arbitrário das próprias razões - Art. 345 do C.P.)

ASPECTOS JURÍDICOS E ÉTICOS DE SIC

5) Bitknapping: “rapto” de dados e ameaça de destruição se não houver pagamento em dinheiro (Extorsão - Art. 158 do C.P.)

6) Criar uma comunidade *online* que fale mal de religiões (Escárnio por motivo de religião - Art. 208 do C.P.)

7) Mandar e-mail com informações sigilosas para terceiros (Violação de segredo profissional - Art. 154 do CP)

8) Reproduzir software sem autorização com fim comercial (Pirataria - Art. 12 da Lei 9.609/98)

ASPECTOS JURÍDICOS E ÉTICOS DE SIC

9) Empregar meio fraudulento para desviar clientela de outrem (desviar usuário da página da concorrente) (Concorrência desleal - Art. 195 da Lei 9.279/96)

10) Instalar câmeras e transmitir na internet em tempo real cenas de sexo explicito (Ato obsceno - Art. 233 do C.P)

11) Subtrair dinheiro de conta-corrente por meio de transferência via internet, sem autorização do titular da conta (Furto qualificado mediante fraude - Art. 155 § 4º inciso II do C.P.) – se não subtrair dinheiro estelionato (art. 171)

12) Alterar ou destruir dados essenciais ao funcionamento do sistema (Dano - Art. 163 do C.P.)

ASPECTOS JURÍDICOS E ÉTICOS DE SIC

13) Criar página na internet praticando, induzindo ou incitando a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional (Crimes de preconceito - Caput e §2º do art. 20 da Lei 7.716/89)

14) Subtrair software de outrem por meio da invasão de um sistema quebrando bloqueios de firewalls e outros mecanismos de segurança (Furto qualificado - Art. 155, § 4º, inc. I do C.P.)

15) Falsificar cartão de crédito (cartão clonado) com o uso de computadores ou falsificar documentos eletrônicos de caráter pessoal (Falsificação de documento particular - Art. 298 do C.P.) – crime meio

16) Pichar website gerando prejuízos econômicos (Crime de dano - Art. 163 do C.P.)

ASPECTOS JURÍDICOS E ÉTICOS DE SIC

17) Montar página de comércio eletrônico de mercadorias para lavar os lucros de outros delitos ou fazer sucessivas transferências em home bank (Crime de lavagem de dinheiro - Art. 1º da Lei 9.613/98)

18) Vender produtos na internet descrevendo a mercadoria de maneira enganosa ou receber o dinheiro e não entregar o produto Estelionato - Art. 171 do CP

19) Denunciar alguém falsamente em conversa on-line com várias pessoas (Calúnia - Art. 138 do C.P.)

20) Dar *forward* para várias pessoas de um boato eletrônico (Difamação - Art. 139 do C.P.)

ASPECTOS JURÍDICOS E ÉTICOS DE SIC

21) Enviar um *e-mail* para alguém ofendendo sua dignidade ou decoro (Injúria - Art. 140 do C.P.)

22) Cyberstalking (Ameaça - Art. 147 do C.P.)

23) Reproduzir obra intelectual, sem autorização expressa do autor e sem citar a fonte (Violação ao direito autoral - Art. 184 do C.P.)

24) Apresentar, produzir, vender, fornecer, divulgar ou publicar, por qualquer meio de comunicação, inclusive rede mundial de computadores ou internet, fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente (Pedofilia - Art. 241 da Lei 8.069/90)

25) Reproduzir programa de computador, no todo ou em parte, para fins de comércio, sem autorização expressa do autor ou de quem o represente (Violação de direitos autorais de programa de computador - Lei 9.609/98, art. 12)

26) Estabelecer ou explorar jogo de azar na internet mediante o pagamento de entrada ou sem ele (Contravenção de Jogos de Azar - Art. 50 do Decreto-lei 3.688/41)

ASPECTOS JURÍDICOS E ÉTICOS DE SIC

MS 13.677/DF (Julgamento em 05/08/09)

Demissão por repasse de senha de computador a terceiro para assinatura de ponto é legal

A demissão de servidor que cede sua senha pessoal a terceiro com o objetivo de burlar o controle eletrônico de ponto não é desproporcional nem irrazoável. A decisão da Corte Especial do Superior Tribunal de Justiça (STJ) mantém sanção imposta a técnico judiciário do próprio Tribunal.

O relator acrescentou que, em relação ao excesso na pena aplicada, ele não existiria. O ministro Noronha afirmou que a pena proposta pelo MPF – suspensão de 30 dias – seria cabível ao servidor que, após ingressar no Tribunal e registrar no ponto eletrônico sua entrada, se ausentasse, deixando de trabalhar as horas lançadas. Mas, no caso, a situação fora mais grave: o repasse a terceiros da senha que dá acesso ao sistema eletrônico expõe a riscos as informações do Tribunal, atualmente armazenadas, em sua maioria, em meios digitais.

"Ora, nada obstante o intento do impetrante de auferir vencimentos sem a respectiva contra-prestação de serviços – fato que por si é grave, pois denota a intenção de lesar a administração pública (no caso, empregador) –, não se pode desconsiderar que o impetrante deixou a descoberto a segurança do sistema de informática do STJ, a que tinha acesso em razão das atribuições de seu cargo. Daí o porquê de o fato amoldar-se perfeitamente ao estabelecido nas disposições do artigo 132, IX, da Lei n. 8.112, de 1990", entendeu o ministro."

Como esse dispositivo prevê de forma específica a pena de demissão e dispensa a comprovação de dano efetivo – não importaria a amplitude do acesso aos sistemas garantida pela senha ou o efetivo acesso a dados sigilosos –, não seria possível a aplicação do princípio da proporcionalidade. "O princípio da proporcionalidade serve para dosar a pena a ser aplicada, mas não para descaracterizar o tipo a que os fatos se subsumem", concluiu o relator.

ASPECTOS JURÍDICOS E ÉTICOS DE SIC

Uso indevido de e-mail da empresa é motivo para dispensa por justa causa

A 1ª Turma do TRT (Tribunal Regional do Trabalho) da 10ª Região (Distrito Federal e Tocantins) manteve sentença que considerou que ao usar e-mail da empresa onde trabalha, a funcionária pode ser dispensada por justa causa.

Segundo publicou o tribunal, uma atendente de empresa de telefonia recorreu à Justiça do Trabalho com o objetivo de impugnar sua demissão por justa causa. Ela alegava que a empresa teria usado cópias de e-mails para justificar a dispensa, procedimento que seria proibido pela Constituição Federal.

(...) Para o magistrado, o e-mail corporativo não é um benefício contratual indireto. Portanto não há como reconhecer a existência de direito à privacidade na utilização de equipamentos concebidos para a execução de funções geradas por contrato de trabalho. Os juízes da 1ª Turma concluíram que a utilização das mensagens como prova é legítima e ratificaram a demissão por justa causa.

Fonte: http://ultimainstancia.uol.com.br/noticia/48021.shtml - 28/02/2008

SERVIDOR: LEI 8.112/90 – Art. 132: Pena de demissão para o servidor que revelar segredo do qual se apropriou em razão do cargo ou função pública)

Lei nº 8.027/90 (Normas de conduta dos servidores públicos civis da União, das Autarquias e das Fundações Públicas)

Art. 5º, Inc. I: Pena de demissão para o servidor que se valer ou permitir dolosamente que terceiros tirem proveito de informação obtida em função do cargo, para lograr proveito pessoal ou de outrem;

ASPECTOS JURÍDICOS E ÉTICOS DE SIC

BREVES COMENTÁRIOS SOBRE O MONITORAMENTO

Segundo a Polícia Civil de São Paulo, 95% dos casos em que foram identificadas infecções por códigos maliciosos tiveram como origem e-mails corporativos.

O e-mail funcional e a própria internet, segundo entendimento consagrado pela jurisprudência dos Pretórios, não são obrigações contratuais, mas meras ferramentas de trabalho, cabendo a cada órgão definir sua utilização. Portanto, sujeitos a monitoramento, desde que se dê ciência ao usuário (servidor) deste procedimento que tem por objeto resguardar a infraestrutura tecnológica e eventuais ações de responsabilidade, haja vista ser objetiva em se tratando de Administração Pública.

Decorrente dessa responsabilidade, que é objetiva, o monitoramento não é apenas um direito do Administrador, mas uma obrigação uma vez que o órgão é responsável pelos danos causados a terceiros decorrentes do mau uso de suas ferramentas de trabalho, incluídas aí as tecnológicas, ressalvado o direito de regresso contra o causador do dano que agiu dolosa ou culposamente.

Mas e os e-mails de provedores particulares acessados em estações de trabalhos consideradas ferramentas de trabalho?

Este não poderá ser monitorado, porque o e-mail particular não é funcional mesmo sendo acessado de equipamento funcional. Daí a necessidade de se estabelecerem políticas de acesso à internet onde o acesso ilimitado seja restrito.

Exemplo de Vacina Jurídica

“VOCÊ ESTÁ ACESSANDO A REDE CORPORATIVA DA INSTITUIÇÃO XXX. ESTE AMBIENTE É MONITORADO E É RESTRITO A PESSOAS AUTORIZADAS, COM O USO DE SENHA INDIVIDUAL, INTRANSFERÍVEL E SIGILOSA”

MUITO OBRIGADO

gerson.charbel@planalto.gov.br