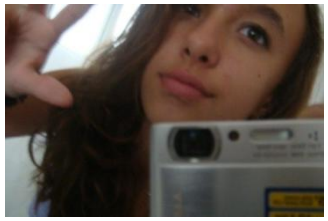
Palestra | 05.03.2013

Workshop sobre a Blindagem Legal da Política e Normas

Apresentação



USP

PECK

Conteúdo Programático

- A Nova Sociedade Digital: Colaborativa e Conectada
- A importância da Proteção da Reputação e do Conhecimento
- A questão da Identidade Digital – Prova de Autoria
- Como fica a Segurança da Informação com a Mobilidade
- Qual o papel do Gestor na Orientação das Equipes
- Limites entre Liberdade de Expressão e o Respeito ao Sigilo Profissional
- Como lidar com Equipes nos ambientes de Redes Sociais
- Monitoramento Corporativo X Privacidade
- Impactos das Novas Legislações em Vigor no Brasil na Gestão e Governança Corporativa
- Principais pontos alterados nos Normativos do Tribunal de Justiça

A Nova Sociedade Digital: Colaborativa e Conectada

http://t1.gstatic.com/images?q=tbn:ANd9GcSfUOQh3V_lAp6SSOJad2PsNK8MhojAhyFPN7b4B7eHNUxq_Hx3 Acessado em 27.02.2013 às 13:31

A Sociedade Digital é o mundo conectado em tempo integral

http://2.bp.blogspot.com/-1P07RbBCZ2Y/UA1QtmF48GI/AAAAAAAABfA/MTxakATXYHs/s1600/cultura-digiyal_Blog.jpg Acessado em 27.02.2013 às 11:43.

Compartilhamento do Conhecimento e Acesso Irrestrito à informação

http://3.bp.blogspot.com/_iBhLHzhUCK8/SI511k9sZ8I/AAAAAAAAA6U/-V0lj6pXYv4/s400/book_3032_big.jpg+(imagem+JPEG,+415x600+pixels)_1243906320985.png
Acessado em 27.02.2013 às 13:25.

Brasil tem 83,4 mi de pessoas conectadas à internet

Por Reuters - Terça-feira, 25 de setembro de 2012 - 14h15

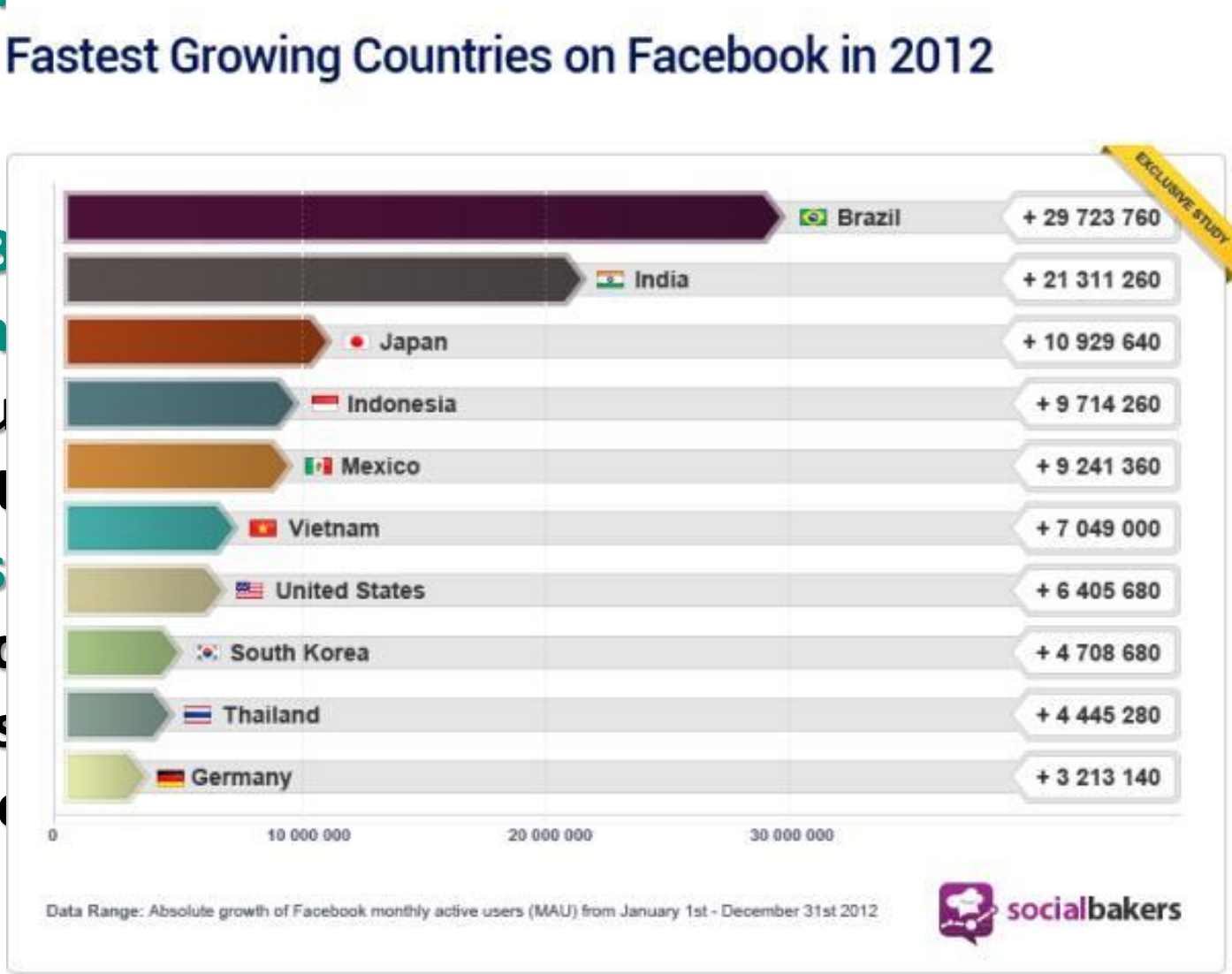
Sxc.hu

Brasil tem 83,4 mi de pessoas conectadas à internet

São Paulo - O número de brasileiros com acesso à Internet atingiu recorde de 83,4 milhões no segundo trimestre deste ano, informou nesta terça-feira o Ibope Nielsen Online.

Se considerados os acessos apenas no local de trabalho ou em residências, o número de usuários chegou a 70,9 milhões em agosto, crescimento de 16 por cento em 12 meses.

http://info.abril.com.br/noticias/internet/brasil-tem-83-4-mi-de-pessoas-conectadas-a-internet-25092012-33.shl Acessado em 27.2.2013 às 13:52.



"O B mero de n ano, segu me o relat .760 bras ocial criac pas a mais com pouc

http://www.tecmund .02.2013 às 13:56.

Nova Sociedade Digital

http://1.bp.blogspot.com/_LNICjasURb8/SuiLKPPO0uI/AAAAAAAAAIo/qvbfI4xoyMk/s400/redes_sociais.jpg
Acessado em 27.02.2013 às 14:05.

Qual a primeira coisa que uma pessoa da era digial faz quando acorda?

62% checa o celular!

47% verifica os emails

29% acessa o Facebook

18% acessa o Twitter

Fonte: http://pinterest.com/pin/35465915785877323/ acesso em 28/05/2012

REVISTA VEJA SÃO PAULO

- ✓ Crianças brasileiras são as que entram mais cedo na web: **aos 9 anos.**
- ✓ Maitê, tem 8 anos, ganhou um videogame aos 4 anos, um celular aos 6 e um notebook aos 7.

Fonte: Revista Veja SP (http://vejasp.abril.com.br/materia/criancas-tecnologia), Agência RS (http://www.agenciars.com.br/blog/criancas-brasileiras-sao-as-que-entram-mais-cedo-nas-redes-sociais/), acesso em 16/10/2012 às 10h01. Foto: Fernando Moraes

E já há também uma geração de pais e famílias mais digitais também!

Fonte: Imagem:http://blig.ig.com.br/vimer/files/2010/01/Casal-Internauta.jpg

Estamos em um contexto de:

Inovação

Mudança de Cultura

Acesso irrestrito à Informação

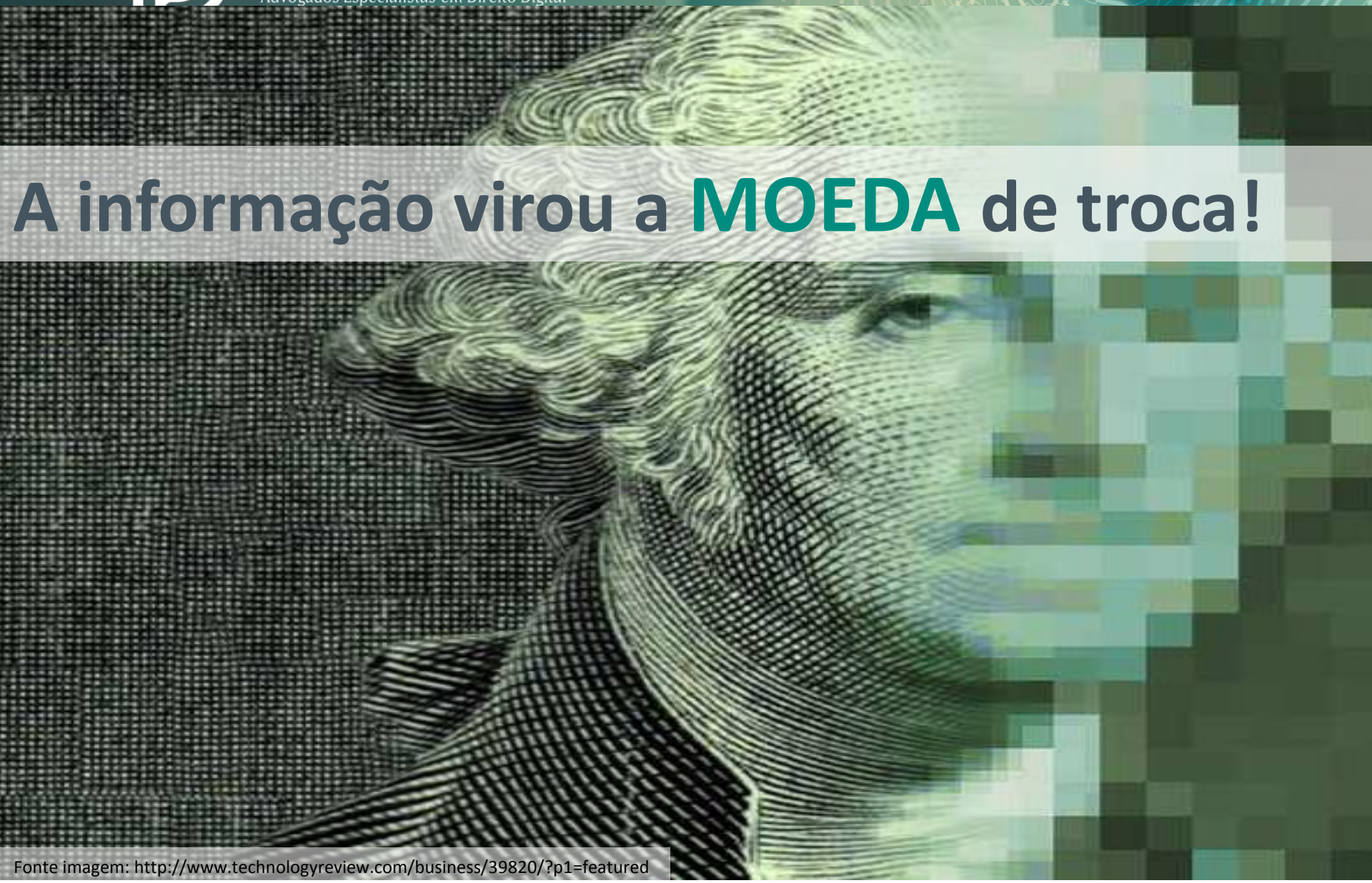
O que será que tem mais valor?

Paradigmas

Novos riscos

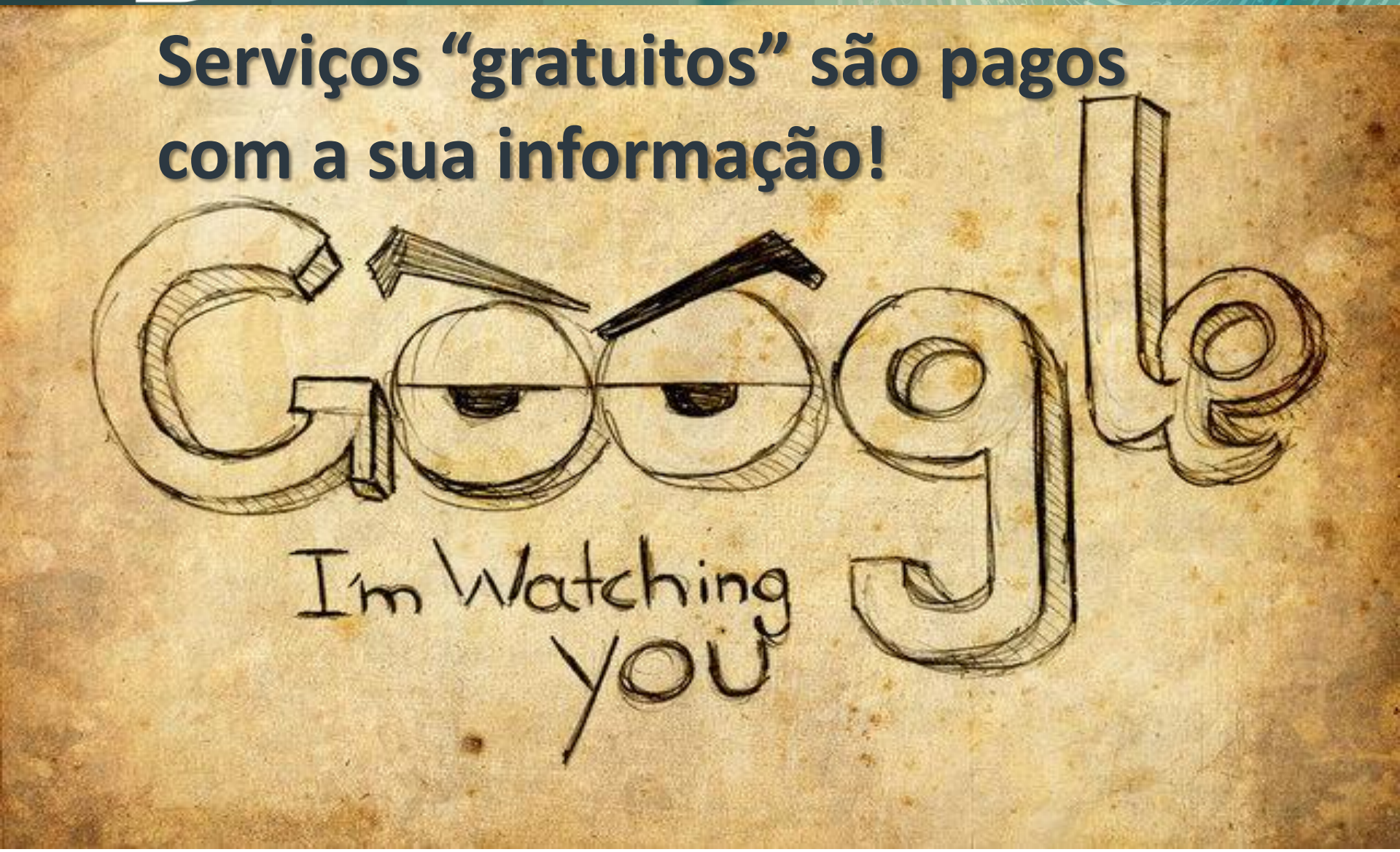
http://3.bp.blogspot.com/-VsNzSeZXWC0/T0z5y3QoqCI/AAAAAAAAAdY/35FPQIOtCp4/s320/mudanca1.jpg Acessado em 07.2.2013 às 10:59.

A informação virou a MOEDA de troca!



Fonte imagem: http://www.technologyreview.com/business/39820/?p1=featured

Serviços “gratuitos” são pagos com a sua informação!



Fonte imagem: http://www.neowin.net/images/uploaded/google_is_watching_you_by_drnour-d46iv7k.jpg

Google Gmail, seção 11.1:

"Ao enviar, postar ou exibir conteúdo você fornece ao Google uma licença perpétua, irrevogável, mundial, livre de royalties e não exclusiva para reprodução, adaptação, modificação, tradução, publicação, exibição pública e distribuição **de qualquer material que você enviar, postar ou exibir nos Serviços ou através deles**".

Dropbox

"Everything in your Public folder is accessible to anyone online."
Tudo na sua pasta "Public" **é acessível para qualquer pessoa online.**

"The Photos folder automatically creates online galleries. Any image files you move or copy to your Photos folder are automatically included in an online gallery anyone can view from the Dropbox website. "
Na pasta fotos criará galerias online automaticamente. **Qualquer arquivo que você mover ou copiar para esta pasta será exposta e qualquer um poderá ter acesso.**

Fonte: https://www.dropbox.com/help/140/en acesso em 24/08/2012
Imagem: http://en.wikipedia.org/wiki/File:Dropbox_logo.svg

G1 | São Paulo

SÃO PAULO

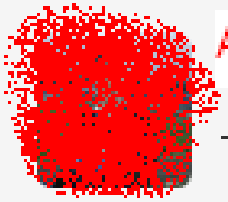
Quadrilha escolhia vítimas para sequestro pela internet, diz polícia

Em SP, grupo manteve estudante de 19 anos em cativeiro por 5 dias. Especialista orienta a usar controles de privacidade das redes sociais.

Já fez o seu check in hoje?

Policiais de São Paulo constataram que uma quadrilha que sequestrou um jovem de 19 anos utilizava a internet para descobrir o perfil e a rotina das vítimas. Ele foi mantido em cativeiro por cinco dias, em Ilha Comprida, litoral sul paulista. De acordo com a polícia, os criminosos passavam horas em sites de relacionamento à procura de pessoas com sinais de riqueza.

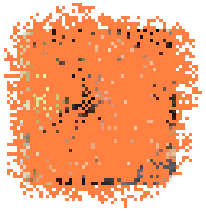
http://www.webdialogos.com/wp-content/uploads/2012/01/logomarca-do-Foursquare-no-Joga_no_google.jpg
http://g1.globo.com/sao-paulo/noticia/2010/08/quadrilha-escolhe-vitimas-para-sequestro-pela-internet-diz-policia.html



Alguém 3h

já **cheguei em casa**, mas minha mãe e meu padrasto sairam pra almoça e agora vou ter que fica esperando o almoço e to morto de fome af

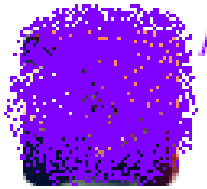
Expand Reply Retweet Favorite



Fulano 1h

@letaccilo não sabe q eu sou lerda nesse quesito kkkk um dia eu melhoro! **To indo viajar** na sexta e chego dia 20! Vamos nos ver qdo eu voltar

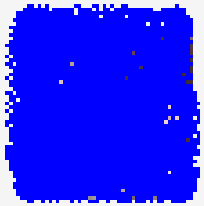
View conversation



Alguém 1h

Cheguei em casa, fui almoçar e depois subi no Bonfa, fui no Banco do Brasil e andei o bairro "todo" pra por créditos p mim e enfim achei.

Expand

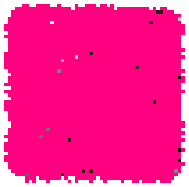


Falo muito!

1 Dec

o povo de **casa** ta **indo viajar** e eu vou ficar sozinha até amanhã de noite <333333333333333 obg vida

Expand Reply Retweet Favorite

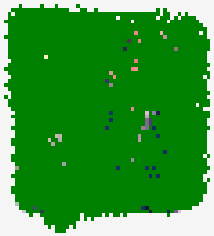


Gosto de falar!

1h

A única parte ruim de ser filha única é que se você passa mal **em casa** de tarde tipo hoje, **não tem ninguém** para te ajudar :(

Expand



Me liguem!

28 Nov

To **indo** pra **escola**, me chamem no whats ou sms! 9[redacted]

Expand Reply Retweet Favorite

E quais são os Desafios Institucionais?

- Inexistência de perímetros
- Abordagem tradicional de SI não é mais suficiente

http://1.bp.blogspot.com/_WTReZvFpd-0/TDuD5Qo-ZUI/AAAAAAAAAGU/RDaD76m5Rq4/s320/inovacao.gif Acessado em 07.02.2013 às 11:33.

- Novas ameaças, como social phishing, mobiles e APTs
- Foco nas Pessoas e não mais na Tecnologia
- Proteção da Informação, esteja ela onde estiver

REGRAS CLARAS
TRANSPARÊNCIA
CONSCIENTIZAÇÃO

Evolução da Prova Escrita

- PEDRA (milhões de anos).

- PAPEL (105 A.C)

Com o passar do tempo, foi possível fazer o registro de fatos com mais mobilidade.

- TELEX (1935)

160 toques. Implantado pela burocracia nazista, serviu a governos, agências de notícia e parentes querendo saudar recém-nascidos.

Fonte: Super Interessante, edição 282, setembro de 2010, pág. 45

Fonte da imagem: http://websigma.com.br/wp-content/uploads/2012/10/evolu%C3%A7%C3%A3o-da-comunica%C3%A7%C3%A3o.jpg

Evolução da Prova Escrita

➢ EMAIL (1968)
Possibilidade de enviar e receber mensagens por sistemas eletrônicos de comuni

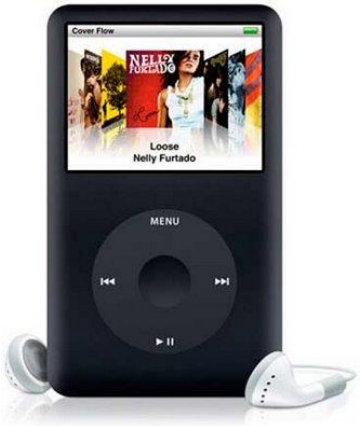
Documentamos por escrito nossa existência há milhares de anos!!

Cada 160 toques geram um torpedo (dados com mobilidade).

➢ TWITTER (2003)
Cada 140 toques geram um tuíte.

Fonte: Super Interessante, edição 282, setembro de 2010, pág. 45

Quando a Sociedade muda...



O DIREITO tem que mudar, EVOLUIR!

O que é o Direito Digital?

O Direito Digital é a evolução do próprio Direito.

O Direito Digital representa o amadurecimento do papel do jurídico como elo entre inovação e gestão.

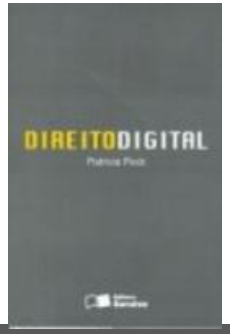
http://3.bp.blogspot.com/-Zs0S4pCLxLc/TVSegSGJHTI/AAAAAAAAABY/BL5Am5MDoHk/s1600/figura_evolucao.jpg Acessado em 14.02.2013 às 11:27.

- ✓ 2001 - Criação da visão **Direito Digital** (como um upgrade do Direito, transversal, multidisciplinar e não mais uma disciplihna ou área vertical como era tratado antes – computerlaw, cyberlaw, direito eletrônico.

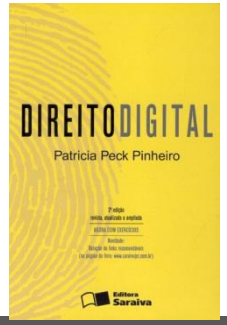
- ✓ A visão trouxe a criação do **4º Elemento**: o **TEMPO** na teoria tridimensional tradicional do Direito (FATO-VALOR-NORMA), essencial para o fundamento do Direito Digital (instantaneidade, autorregulamentação, técnico).

- ✓ Aplicação prática: **mudança de tempo e espaço gerou os trabalhos de eliminação do papel nas relações (desmaterialização completa do suporte – vai de PI a Paperless – atemporal).**

2001 (1ª Ed)

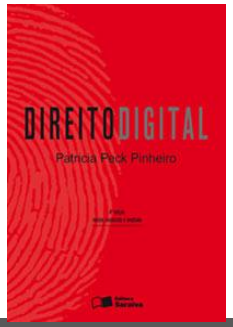


2007 (2ª Ed)



2009 (3ª Ed)

2011 (4ª Ed)



2013 (5ª Ed)

STJ, REsp n.º 1308830/RS, Ministra Nancy Andrighi, terceira turma, 08/05/2012, DJE 18/05/2012.

(...) **Patrícia Peck** comunga dessa ideia e apresenta exemplo que se amolda perfeitamente à hipótese dos autos. A autora considera "tarefa hercúlea e humanamente impossível" que "a empresa GOOGLE monitore todos os vídeos postados em seu sítio eletrônico 'youtube', de maneira prévia", mas entende que "ao ser comunicada, seja por uma autoridade, seja por um usuário, de que determinado vídeo/texto possui conteúdo eventualmente ofensivo e/ou ilícito, deve tal empresa agir de forma enérgica, retirando-o imediatamente do ar, sob pena de, daí sim, responder de forma solidária juntamente com o seu autor ante a omissão praticada (art. 186 do CC)" (Direito digital. 4ª ed. São Paulo: Saraiva, 2010, p. 401)." (STJ, REsp 1308830/RS, Rel. Ministra NANCY ANDRIGHI, TERCEIRA TURMA, julgado em 08/05/2012, DJE 18/05/2012).

STJ, REsp n.º 1,186.616/MG, Ministra Nancy Andrighi, terceira turma, 31/08/2011.

"APELAÇÃO CÍVEL - INFORMAÇÕES OFENSIVAS POSTADAS NO INTERNET - RESPONSABILIDADE DO PROVEDOR - RETIRADA IMEDIATA DA PÁGINA DO AR APÓS COMUNICAÇÃO - AUSÊNCIA - DANOS MORAIS CONFIGURADOS - INCIDÊNCIA DO CÓDIGO DE DEFESA DO CONSUMIDOR. - A exploração comercial da internet configura relação de consumo e está sujeita aos dispositivos previstos na Lei nº 8.078/90. - "Como afirma **Patricia Peck,** a fiscalização prévia, pelo provedor de conteúdo, do teor das informações postadas na web por cada usuário não é atividade intrínseca ao serviço prestado, de modo que não se pode reputar defeituoso, nos termos do art. 14 do CDC, o site que não examina e filtra os dados e imagens nele inseridos. O dano moral decorrente de mensagens com conteúdo ofensivo inseridas no site pelo usuário não constitui risco inerente à atividade dos provedores de conteúdo, de modo que não se lhes aplica a responsabilidade objetiva prevista no art. 927, parágrafo único, do CC/02. Ao ser comunicado de que determinado texto ou imagem possui conteúdo ilícito, deve o provedor agir de forma enérgica, retirando o material do ar imediatamente, sob pena de responder solidariamente com o autor direto do dano, em virtude da omissão praticada" (STJ, REsp. 1.186.616 - MG, Rel. Min. Nancy Andrighi, 31/08/2011).

STJ, REsp n.º 1.193.764 - SP, Ministra Nancy Andrighi, 14/12/2010.

Patrícia Peck comunga dessa ideia e apresenta exemplo que se amolda perfeitamente à hipótese dos autos. A autora considera "tarefa hercúlea e humanamente impossível" que "a empresa GOOGLE monitore todos os vídeos postados em seu sítio eletrônico 'youtube', de maneira prévia", mas entende que, "ao ser comunicada

TJ-MG, Apelação Cível n.º 0456532-68.2010.8.13.0024, Relator José Marcos Vieira, 11/05/2011.

"Mais uma vez, importante a lição de **PATRÍCIA PECK PINHEIRO**, sobre responsabilidade civil no direito digital: Considerando apenas a Internet, que é mídia e veículo de comunicação, seu potencial de danos indiretos é muito maior que de danos diretos, e a possibilidade de causar prejuízo a outrem, mesmo que sem culpa, é real. Por isso, a teoria do risco atende às questões virtuais e a soluciona de modo mais adequado devendo estar muito bem associada à determinação legal de quem é o ônus da prova em cada caso.

TJ-SP, Agravo de Instrumento 584.783.4/7-00, Relator Egidio Giacoia, 02/12/2008

Aqui, vale transcrevermos as lições de **PATRÍCIA PECK PINHEIRO** "in" Direito Digital, Saraiva, 2a Ed./2001, p. 123, sobre os provedores de hospedagem.

TRT 2ª, Acórdão n.º2006 0395367, Relator: Dr. Valdir Florindo, 09/06/2006

Para se ter uma ideia da repercussão do site 'orkut', bem como de seus males, válido transcrever o posicionamento de **Patrícia Peck**, autora do livro 'Direito Digital', em seu artigo 'Os males do Orkut e outros males da Tecnologia': "A internet não é simplesmente uma rede de computadores, é sim uma rede de pessoas, e como tal, está sujeita às leis vigentes nos países nos quais as pessoas se encontram. Como toda e qualquer tecnologia, pode ser usada para o bem, ou para o mal. A questão da ética e da legalidade, no uso das tecnologias é antiga no Direito.

A importância da Proteção da Reputação e do Conhecimento

http://t1.gstatic.com/images?q=tbn:ANd9GcSfUOQh3V_lAp6SSOJad2PsNK8MhojAhyFPN7b4B7eHNUxq_Hx3 Acessado em 27.02.2013 às 13:31

A Reputação e o Conhecimento são os ativos mais importantes na Sociedade Digital!

http://1.bp.blogspot.com/-9LEfNpJ33UE/TduJ-f2Kx9I/AAAAAAAAAXw/44MS0QIRNXo/s1600/594738_email_marketing.jpg
Acessado em 27.02.2013 às 14:45.

Proteção da Reputação

No ultimo domingo (3.3), a conta do Ministério da Defesa no Twitter, usada para comunicar sobre a agenda do órgão, publicou um recorde do game "Banana Kong". O erro fez com que a mensagem fosse retuítada por mais de 3 mil usuários do microblog antes de ser apagada. Segundo o Ministério da Defesa "foi identificado um erro no manuseio do tablet particular de um servidor da área de monitoramento de redes sociais da pasta. Este erro teria gerado uma publicação automática no perfil do ministério no Twitter."

http://epocanegocios.globo.com/Revista/Common/0,,EMI130181-16349,00-MENSAGEM+NO+TWITTER+CAUSA+DEMISSAO+DE+EXECUTIVO+DA+LOCAWEB.html Acessado em 27.02.2013 às 14:54.

Vaticano: Twitter está proibido durante o conclave

Religiosos querem evitar comentários e vazamento de informação até a escolha do novo Papa.

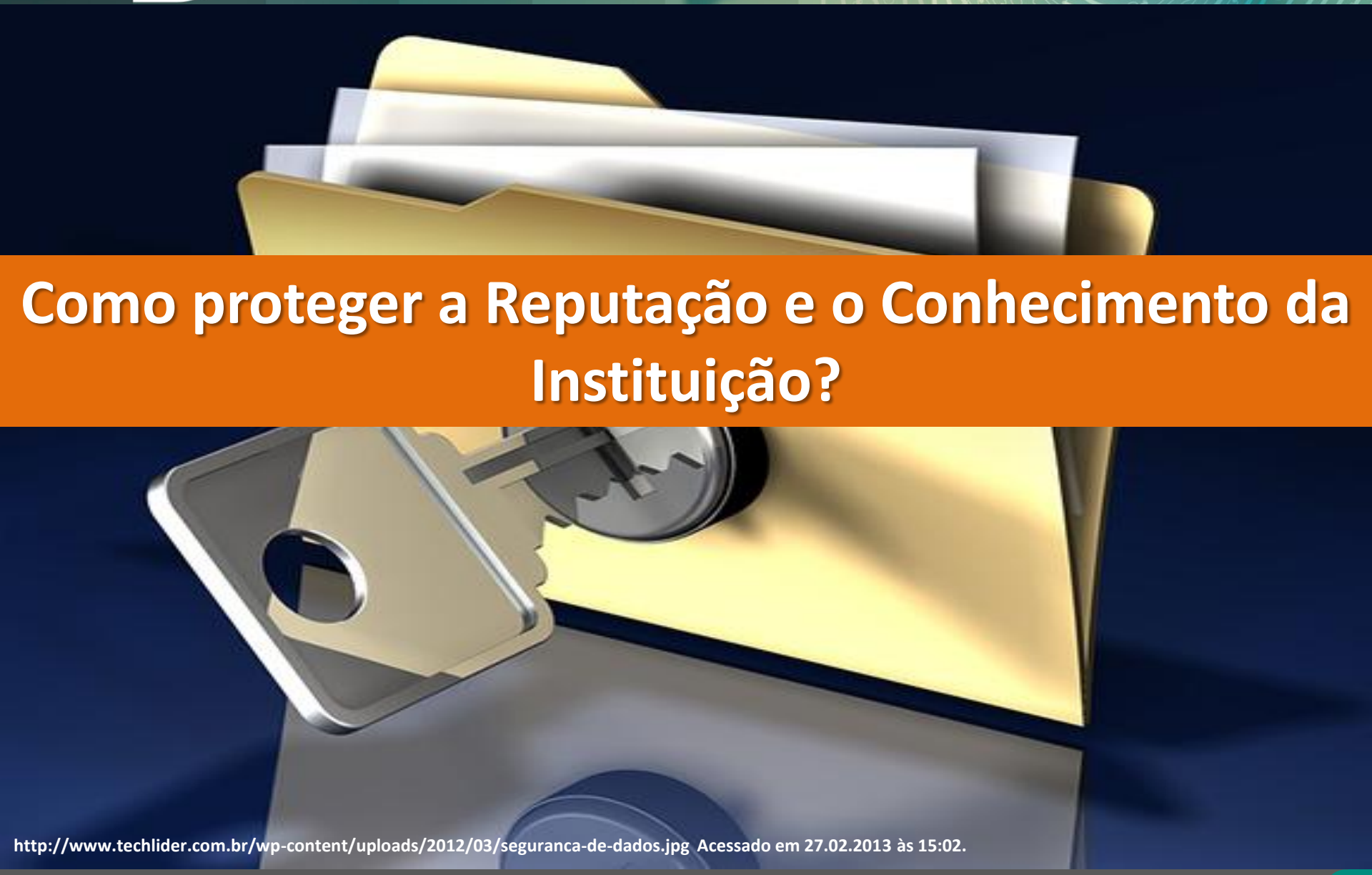
Tweet 12 | Curtir 34 | +1 4 | 2 | 1.781 visualizações

Por Rafael Gazzarrini em 19 de Fevereiro de 2013

Religiosos querem evitar comentários e vazamento de informação até a escolha do novo Papa.

Twitter do cardeal brasileiro Odilo Scherer. (Fonte da imagem: Reprodução/Twitter)

Com a renúncia do Papa Bento XVI, muitas teorias da conspiração surgiram, mas o único fato concreto dessa história toda é que um novo pontífice deve ser escolhido para comandar a Igreja Católica. Esse processo de escolha é chamado de conclave, sendo que ele costuma levar centenas de devotos até o Vaticano.



Como proteger a Reputação e o Conhecimento da Instituição?

http://www.techlider.com.br/wp-content/uploads/2012/03/seguranca-de-dados.jpg Acessado em 27.02.2013 às 15:02.

O que a Instituição pode fazer?

- Monitorar a marca da instituição na internet e nas Mídias Sociais;
- Planejar e gerenciar a participação na internet e nas Mídias Sociais;
- Realizar campanhas de conscientização;
- Estar atento ao canal de comunicação utilizado – cada um tem uma linguagem distinta;
- Ser transparente. Em caso de informação ou comentário negativo, responda rapidamente;
- Gerar sempre conhecimento e conteúdo positivo.

O que o colaborador ou agente judiciário deve fazer?

- Evitar associar CONTEÚDO PESSOAL ou de OPINIÃO PARTICULAR com a Marca da Instituição;
- Zelar pelo sigilo profissional e evitar publicar informações de ROTINA DE TRABALHO;
- Realizar COMPARTILHAMENTO SEGURO de informações e não vazar conhecimento;
- Ser discreto, diligente e evitar excesso de exposição vida íntima;
- Praticar liberdade de expressão com RESPONSABILIDADE;
- Publicar opiniões baseadas na BOA-FÉ e em conformidade legal;
- Evitar linguagem subjetiva e ofensas digitais;
- Usar apenas imagens e/ou fotos que tenha sido autorizado;
- Somente utilizar conteúdos que tenha LEGITIMIDADE ou que seja AUTOR ou que tenha tido AUTORIZAÇÃO PRÉVIA.

Norma de Utilização de Ativos de Informação e Recursos de Tecnologia da Informação e Comunicação

5.3.2. O agente judiciário ou colaborador não deve acessar, armazenar, utilizar, compartilhar ou transmitir qualquer informação, conteúdo ou recurso indevido quando da utilização de recursos de TIC do TJPE, que forem:

5.3.2.1. - Impróprios ou que atentem contra a legislação vigente, a moral, a ética ou as normas da instituição;

5.3.2.4. - Que representem uma quebra de sigilo das informações do TJPE.

Lei nº 6.123 de 20 de julho de 1968 – Estatuto do Funcionário Público de Pernambuco

Art. 193. São deveres do funcionário, além do desempenho das tarefas cometidas em razão do cargo ou função:

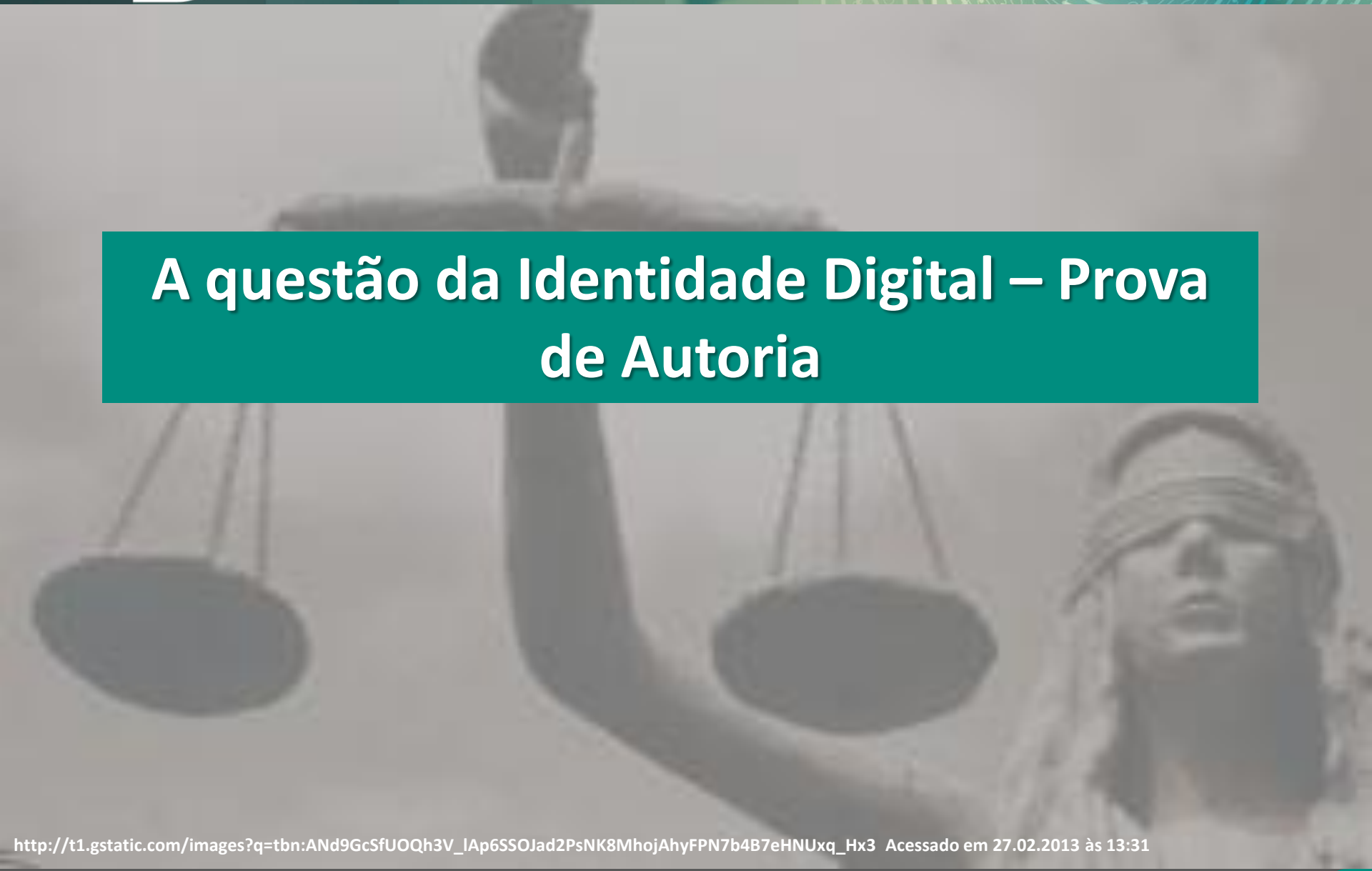
VII - observância às normas legais e regulamentares;

XII - guardar sigilo sobre documentos e fatos de que tenha conhecimento em razão do cargo ou função.

Proteção da Reputação

Proteja a sua Reputação Digital!

A questão da Identidade Digital – Prova de Autoria



http://t1.gstatic.com/images?q=tbn:ANd9GcSfUOQh3V_lAp6SSOJad2PsNK8MhojAhyFPN7b4B7eHNUxq_Hx3 Acessado em 27.02.2013 às 13:31

A identidade Digital possibilita a identificação da autoria e evita o anonimato.

http://www.techlider.com.br/wp-content/uploads/2009/12/identidade-digital.jpg Acessado em 14.02.2013 às 15:41.

A autenticação é um processo que permite a verificação, para posterior validação, de determinada Identidade Digital.

1 - http://www.sucataeletronica.com.br/style/images/informatica/token.jpg
2 - http://images03.olx.com.br/ui/19/22/91/1357648029_470392191_1-Leitora-cartao-inteligente-certificado-digital-BH-e-CNPJ-e-CPF-OAB-CAIXA-CEF-Funcionarios.jpg
3 - http://www.bibliosys.com.br/uploads/informativo/1308/original_biometria.jpg
4 - http://www.porvoce.com.br/img/help/login.png

Acessados em 14.02.2013 às 15:56.

DIREITO CIVIL. INSTITUIÇÃO BANCÁRIA. CEF. GESTORA DO FGTS. SERVIÇO PÚBLICO. RESPONSABILIDADE CIVIL OBJETIVA. ART. 37, § 6º DA CF/88. EXTRAVIO DE VALORES. **COMPARTILHAMENTO DE SENHA POR FUNCIONÁRIOS**.

1 - A CEF está sujeita aos preceitos da responsabilidade civil objetiva prevista no art. 37, § 6º da Constituição Federal, porquanto **se trata de empresa pública**, com personalidade jurídica de direito privado, que presta, relativamente à gestão do Fundo de Garantia por Tempo de Serviço, um serviço público. 2 - **In casu, o saque fraudulento em conta vinculada do FGTS ocorreu inegavelmente em razão da negligência (disponibilização de senha para compartilhamento)**, porém não atribuível a funcionário que permitiu tal prática ou a quem dela aproveitou, mas sim **à própria CEF, a quem cabia fiscalizar e coibir a execução de atividades por quem não detinha atribuição para tal, possibilitada em razão da prática disseminada, dentro de seu estabelecimento, de compartilhamento de senha.** 3 - A CEF não comprovou o desconhecimento da prática do "compartilhamento de senha", nem que o Réu XXX **tivesse assinado um termo de responsabilidade no qual assumiria que a senha era pessoal e intransferível, o que evidencia a negligência de sua conduta.** 4 - Apelação conhecida e improvida.

PROCESSO Nº TRF-2-200051010154630. SEXTA TURMA ESPECIALIZADA – 17/06/2009.

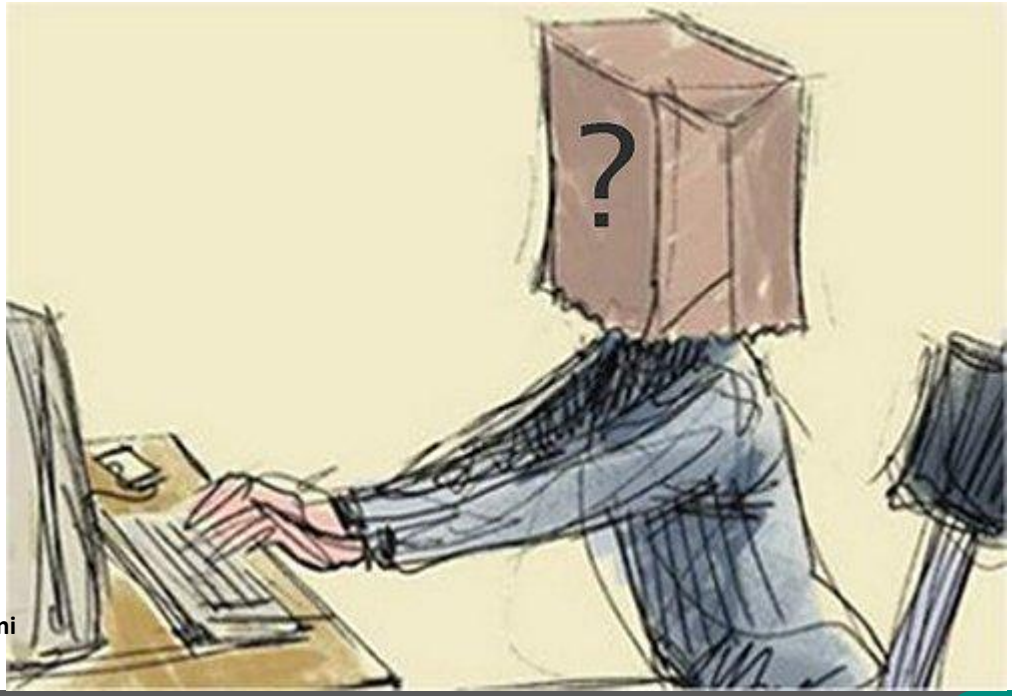
PENAL. PROCESSUAL PENAL. PECULATO-DESVIO. CONCESSÃO FRAUDULENTA DE BENEFÍCIOS PREVIDENCIÁRIOS. FUNCIONÁRIOS DO INSS. DISPONIBILIDADE JURÍDICA DE VALORES PÚBLICOS. MODUS OPERANDI. **USO DE SENHA ELETRÔNICA PESSOAL E INTRANSFERÍVEL.** DESCLASSIFICAÇÃO NÃO CONFIGURADA. ADEQUAÇÃO DA PENA. RECURSOS DESPROVIDOS

O modus operandi dos delitos em questão se realizava por meio eletrônico, dispensando a presença física do agente no exato local de sua lotação, **bastando, para tanto, a posse de senha eletrônica relativa à lotação, com atribuição para habilitação e concessão de benefícios**. 3 - **A possibilidade de uso da senha pessoal e intransferível do acusado por terceira pessoa ou mesmo troca dessa senha sem seu conhecimento cai por terra ante a existência de documentação, a qual atesta não ter ocorrido reinicialização da senha do usuário e não ser possível a existência de duas senhas para uma mesma matrícula.** Ademais, a **responsabilidade pelo sigilo de senhas pessoais é do próprio acusado, mormente em se tratando de senha de uso profissional**, não sendo plausível a escusa de que um terceiro desconhecido dela teria se utilizado, sem que tenha sido produzida prova mínima nesse sentido, como determina o artigo 156 do Código de Processo Penal. Pena adequadamente fixada acima do mínimo legal. 8 – Recursos de apelação desprovidos.

PROCESSO Nº TRF-2-199751010612333. PRIMEIRA TURMA ESPECIALIZADA – 18/08/2010.

A Identidade Digital possibilita a geração de prova de autoria e evita o anonimato

Constituição Federal, Art. 5º, IV - é livre a manifestação do pensamento, sendo vedado o anonimato.



http://www.sindjus.org.br/portal/noticias/fotos_noticias/20121122141855Anonimato2.jpg Acessado em 27.02.2013 às 16:16.

Norma de Controle de Acesso

5.1.3. O acesso aos ativos de informação e recursos de TIC deve ser controlado e restrito aos agentes judiciários e demais colaboradores autorizados pela SETIC, conforme orientação do binômio de necessidade funcional e mais restrita permissão cabível.

Cada um é responsável pela sua Identidade Digital

restrições ao acesso, tais como número de identificação funcional, assinatura manuscrita, certificado digital, combinação de login e senha, uso de token e/ou biometria.

5.1.6. Não é permitido o acesso aos ativos de informação ou uso de qualquer recurso de TIC sem as credenciais de acesso correspondentes.

Norma de Controle de Acesso

5.4.2.1. Não é admissível, sob nenhuma hipótese, o compartilhamento da identidade digital, ou de recurso de TIC que tenha o propósito de autenticação de um agente judiciário ou colaborador para quem quer que seja, a exemplo, mas não se limitando ao nome de usuário e senha, token e certificado digital.

5.6.1. Constitui uso indevido das senhas:

5.6.1.1. Fornecer o login (ID) e senha de qualquer sistema ou recurso de TIC do TJPE para outrem, independentemente do motivo;

5.6.1.2. Utilizar o login (ID) e a senha de outrem para ter acesso aos ativos de informação ou recursos de TIC do TJPE.

Art. 307 CP: Crime de "**Falsa Identidade**":

*Pena - **Detenção, de 3 (três) meses a 1 (um) ano, ou multa**, se o fato não constitui elemento de crime mais grave.*

Lei nº 6.123 de 20 de julho de 1968

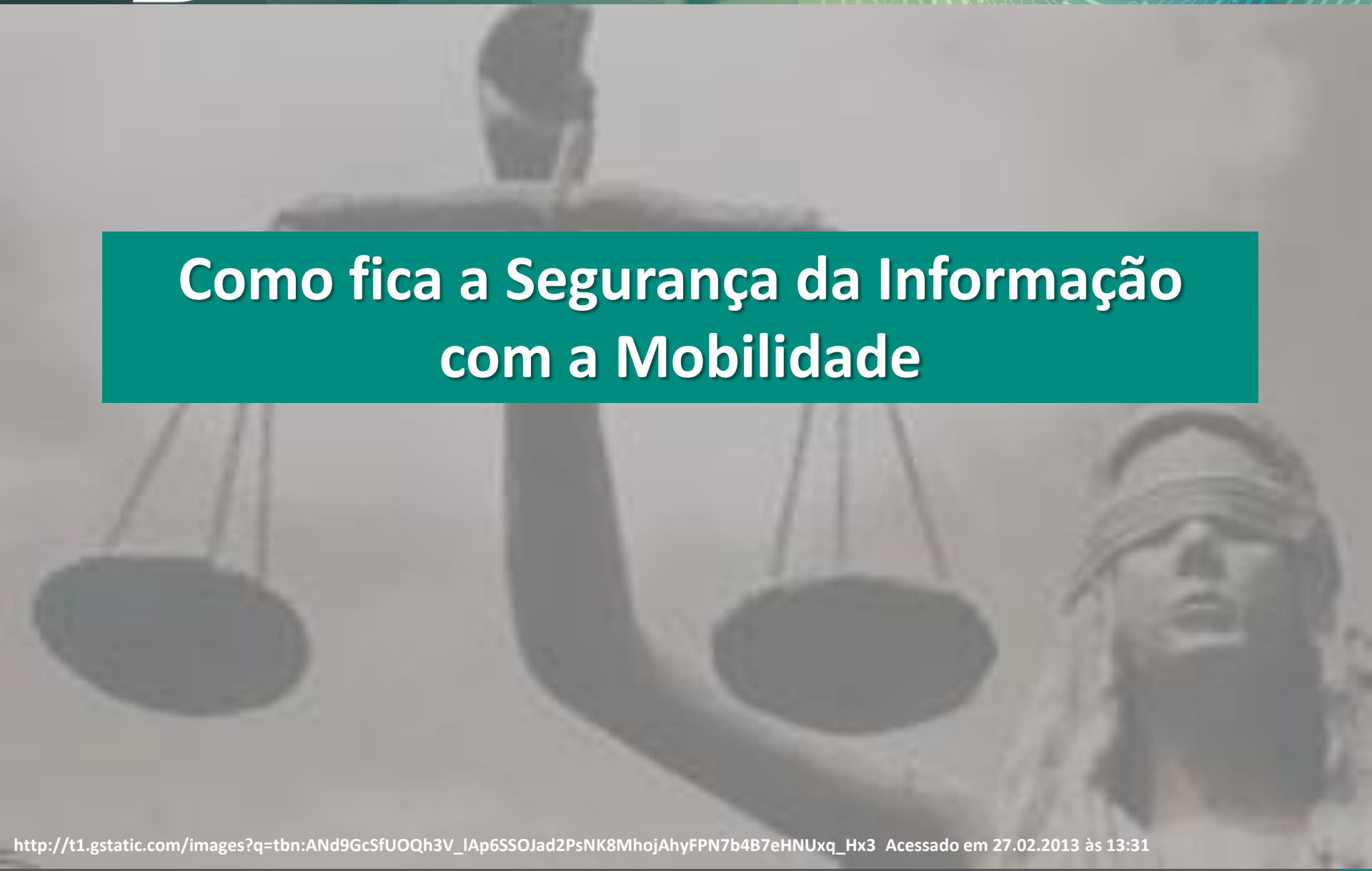
Art. 195. Pelo exercício irregular de suas atribuições, o funcionário responde civil, penal e administrativamente

não constitui crime mais grave.

§ 1º Nas mesmas penas deste artigo incorre quem:

I – permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informações ou banco de dados da Administração Pública.

Como fica a Segurança da Informação com a Mobilidade



http://t1.gstatic.com/images?q=tbn:ANd9GcSfUOQh3V_lAp6SSOJad2PsNK8MhojAhyFPN7b4B7eHNUxq_Hx3 Acessado em 27.02.2013 às 13:31

A mobilidade trouxe riscos novos e desconhecidos

http://4.bp.blogspot.com/_F6U-a6cr6fg/TKJaHihxKaI/AAAAAAAAAIs/DoxZnsRKEYI/s1600/Gerenciamento+dos+riscos.jpg Acessado em 14.02.2013 às 14:29.

"Pesquisadores do Laboratório da ESET na América Latina apresentam um balanço dos principais problemas de segurança identificados na região durante este ano"

"O vazamento de informações liderou os incidentes relacionados à segurança da informação na América Latina em 2012, de acordo com relatório divulgado pelo laboratório da ESET. **O mesmo documento destaca os ataques voltados a explorar vulnerabilidades nos smartphones como a segunda maior causa de problemas relacionados ao cibercrime**.

No mundo, entre os casos mais importantes de vazamento de informações neste ano está o roubo de dados de mais de 56 mil clientes da Visa e Mastercard, a exposição de 6,5 milhões de senhas do Linkedin e mais de 450 mil credenciais roubadas do Yahoo! Voice."

http://www.jornalbrasil.com.br/index.php?pg=desc-noticias&id=64848 Acessado em 27.02.2013 às 16:40.

http://olhardigital.uol.com.br/negocios/digital_new ... la-mobilidade-pode-exceder-o-da-internet,-afirma-estudo Acessado em 25.02.2013 às ...

Impacto da mobilidade pode exceder o da internet, afirma estudo

Dois terços dos executivos de TI acreditam que a mobilidade terá um impacto tão grande ou maior que o surgimento na internet

26 de Junho de 2012 | 18:00h

Compartilhe: 219 0 7 28 A- A+

Impacto da mobilidade pode exceder o da internet, afirma estudo

Um estudo divulgado pela Accenture descobriu que dois terços dos responsáveis pelos departamentos de TI das empresas acreditam que a mobilidade terá um impacto tão grande ou maior que o registado com o surgimento da internet nos anos 90.

Reprodução

Segundo a pesquisa, 67% dos CIOs e executivos de TI estimam que a adoção de soluções de mobilidade "vai impactar os seus negócios igual ou mais do que a internet na década de 1990".

Jurisprudência

"O impetrante discorda sobre deferimento de liminar em "Ação de Obrigação de Não Fazer" ajuizada pela EMPRESA para que o réu (impetrante) se abstenha de imediato, da divulgação e/ou aproveitamento de qualquer informação da empresa em especial daquelas cujo desvio foi apurado por meio de perícia nos autos do Processo Cautelar de Busca e apreensão 1454/10, embora ainda em trâmite(...) réu deverá cumprir as obrigações previstas nas cláusulas sexta, sétima e oitava do contrato firmado com a autora, conforme doc. 05 dos autos do processo 968/11..."

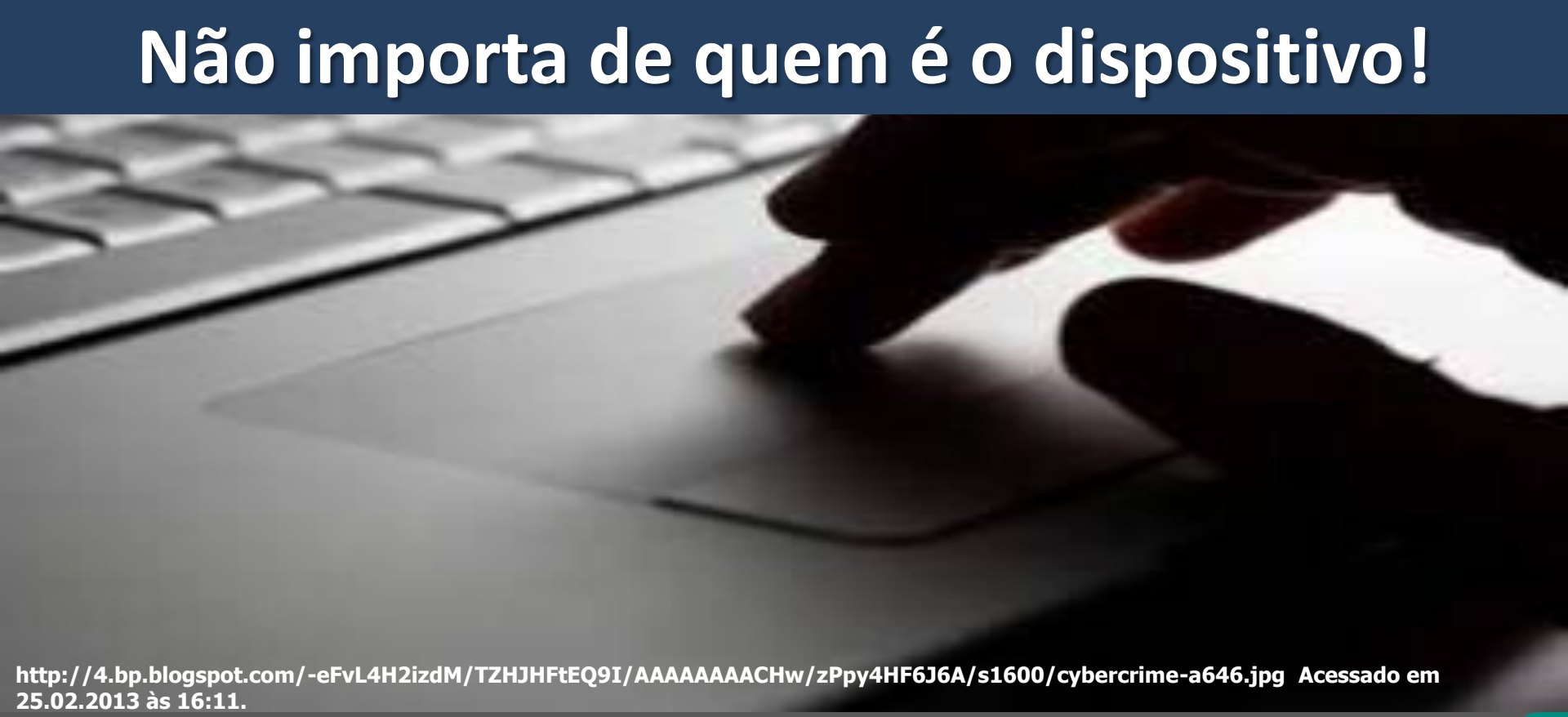
PROCESSO Nº:00046858820115020000 - Mandado de Segurança. Desembargador Relator José Roberto Carolino.

Jurisprudência

"Alega o impetrante que todos os arquivos pertencentes à Empregadora identificados e localizados em seus dois computadores lá estão em função de que se utilizava de tais arquivos para seus serviços cotidianos naquela empresa, e após sua rescisão não promoveu nenhuma atitude que pudesse de alguma forma reproduzir ou utilizar tais arquivos. Na época de sua saída da Empregadora simplesmente não foi solicitado ao mesmo que fossem apagados tais arquivos ou devolvidos, como também, em nenhum momento de seu contrato de trabalho foi imposta qualquer restrição de uso ou cópia de tais arquivos, daí a afirmação de que tais documentos não eram classificados como arquivos sigilosos da Empregadora."

PROCESSO Nº:00046858820115020000 - Mandado de Segurança. Desembargador Relator José Roberto Carolino.

Não importa de quem é o dispositivo!



http://4.bp.blogspot.com/-eFvL4H2izdM/TZHJHFtEQ9I/AAAAAAAACHw/zPpy4HF6J6A/s1600/cybercrime-a646.jpg Acessado em 25.02.2013 às 16:11.

A Segurança das Informações institucionais é um dos grandes desafios no BYOD

http://www.virtue.com.br/blog/wp-includes/images/Data%20Breach.jpg Acessado em 25.02.2013 ás 18:51.

Para garantir a Segurança da Informação no uso dos Dispositivos Móveis:

- Estabelecer controle de acesso adequado às informações institucionais;
- Bloqueio por senha após breve período inatividade;
- Impossibilitar tecnicamente a conexão de dispositivo móvel particular na rede ou recursos institucionais;
- Realizar o monitoramento das informações e dos dispositivos institucionais;
- Instalar softwares de segurança que impossibilitem a alteração de configurações pelo colaborador/agente judiciário;
- Instalar software que permita rastrear o dispositivo em caso de perda, furto ou roubo ou excluir suas informações.

Norma para Dispositivo de Mobilidade e Acesso Remoto

5.3.1. Quando o dispositivo de mobilidade for fornecido pelo TJPE, os agentes judiciários e demais colaboradores devem realizar cuidados básicos de segurança, a exemplo, mas não se limitando ao backup (cópias de segurança) das informações da instituições, varredura de vírus e conectá-lo periodicamente à rede corporativa para atender procedimentos rotineiros de checagem de conformidade.

5.4.1. O dispositivo de mobilidade particular que não faça parte dos ativos do TJPE não deve ser conectado à rede corporativa, salvo se houver expressa autorização da chefia imediata responsável pelo agente judiciário e da SETIC.

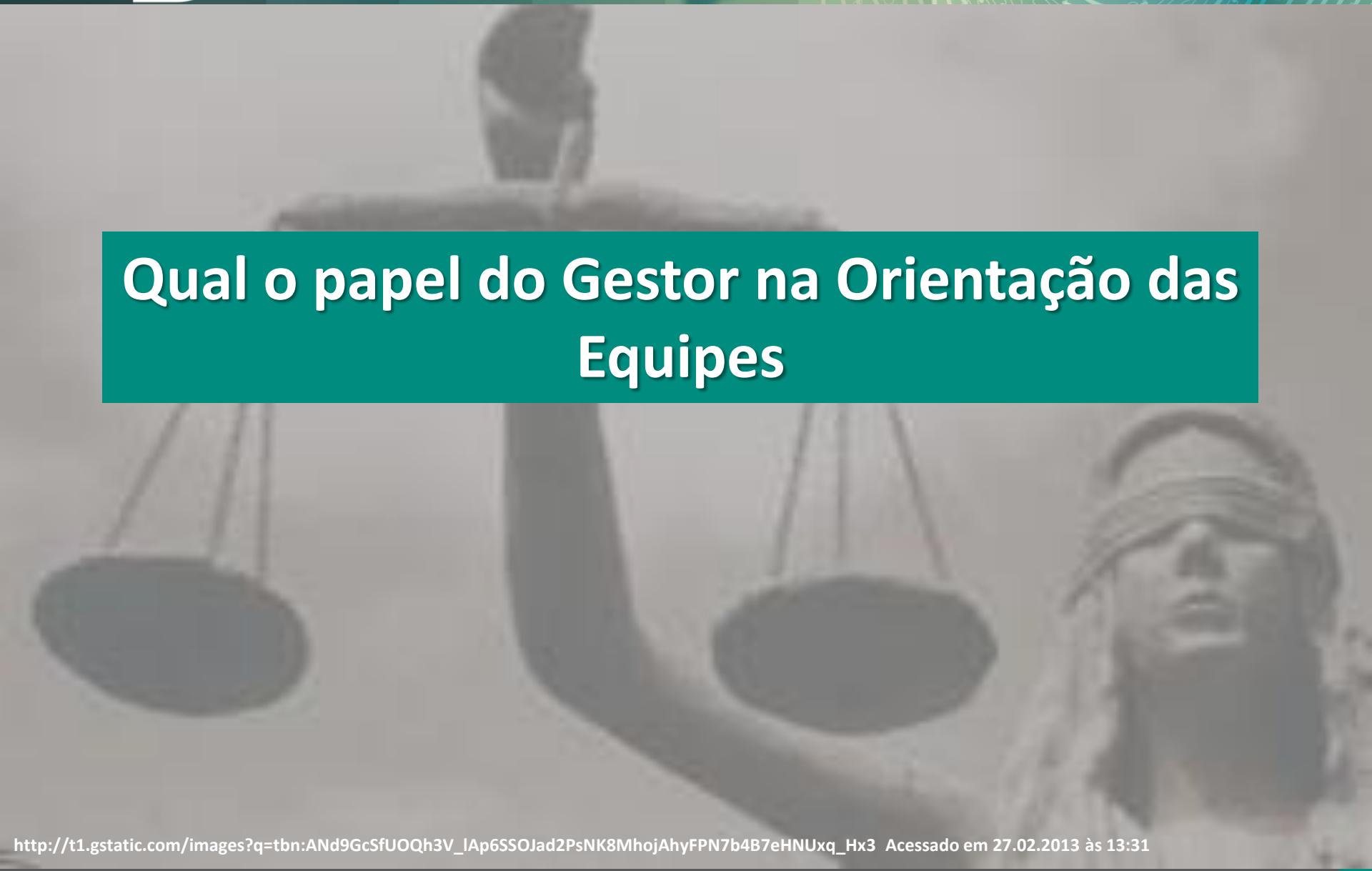
5.4.3. Os agentes judiciários e demais colaboradores que utilizarem dispositivo de mobilidade particular, de qualquer espécie, são responsáveis pelos conteúdos e softwares que armazenarem além das configurações e ferramentas de segurança que utilizarem, podendo ser responsabilizados por qualquer impacto ao TJPE decorrente da exploração de vulnerabilidades dos seus equipamentos.

Norma para Dispositivo de Mobilidade e Acesso Remoto

5.6.1. As informações do TJPE constantes em dispositivos de mobilidade e aquelas acessadas por meio do acesso remoto devem ser protegidas contra acessos indevidos, modificação, destruição, compartilhamento ou divulgação não autorizada. Assim, devem ser aplicados métodos adequados de autenticação e de controle de acesso, incluindo, mas não se limitando a bloqueio automático por senha e/ou mecanismos de criptografia devidamente homologados pelo TJPE.

5.6.2.11. É proibido visualizar, acessar, efetuar o download (baixar arquivos) ou upload (transmitir arquivos), utilizar, instalar, armazenar, divulgar ou repassar qualquer material, conteúdo, ou recurso ilícito, impróprio, obsceno, pornográfico, difamatório, ofensivo, discriminatório, que atente à moral e aos bons costumes, que viole a boa-fé ou que não seja compatível com as diretrizes e interesses do TJPE em dispositivos institucionais.

Qual o papel do Gestor na Orientação das Equipes



http://t1.gstatic.com/images?q=tbn:ANd9GcSfUOQh3V_lAp6SSOJad2PsNK8MhojAhyFPN7b4B7eHNUxq_Hx3 Acessado em 27.02.2013 às 13:31

Papel do Gestor

E qual o papel do Gestor?

http://t0.gstatic.com/images?q=tbn:ANd9GcQKIOuCLvt3wOOTigk6LOvYu7dYJcGxhvCtStONZ3U5AeJtg5Th Acessado em 27.02.2013 às 17:08.

O gestor tem o papel de:

- Fiscalizar, estimular e assegurar o cumprimento das normas internas e da legislação em vigor pelos agentes judiciários e colaboradores sob sua responsabilidade;
- Garantir o livre acesso à comunicação com seus colaboradores e agentes judiciários.

Está na Lei nº 6.123 de 20 de julho de 1968

Art. 193. São deveres do funcionário, além do desempenho das tarefas cometidas em razão do cargo ou função:
VI - obediência às ordens superiores, exceto quando manifestamente ilegais.

http://images.wikia.com/wikia/pt-br/images/5/5c/Lupa.gif Acessado em 28.02.2013 às 16:34.

A melhor forma de garantir o cumprimento das regras é DAR O EXEMPLO!

http://4.bp.blogspot.com/_xsExyAm0lRs/TThuLcUNQ5I/AAAAAAAABDY/cZFdbORxr3M/s1600/educacao021.jpg Acessado em 27.02.2013 às 17:02.

Não fomos educados para a Era Digital!

Ouvimos nossos avós, pais e professores dizerem...

Não abra a porta para estranhos...”
“Não esqueça a porta aberta...”
“Não pegue carona com estranhos...”
Não pegue o que não é seu...”
Diga-me com quem andas que eu te direi quem és...
Não faça justiça com as próprias mãos!

Mas não ouvimos ninguém dizer...

Não abra email de estranhos...
E não esqueça de bloquear o seu computador...
Cuidado com estranhos do outro lado da tela (messenger, chat, email, comunidade)
Não se deve cobiçar o conteúdo do próximo...
Diga-me com quem navegas que eu te direi quem és...
Não faça justiça com o próprio mouse!

EXERCÍCIO

MATRIZ DE ANÁLISE DE INCIDENTE E IDENTIFICAÇÃO DE RESPONSABILIDADES

INCIDENTES x RESPONSABILIDADE

LEVE	MÉDIO	GRAVE	GRAVÍSSIMO
			

LEGENDA	RESPONSABILIDADE	CONSEQUÊNCIA
	Infração ética (não há norma).	Advertência simples para retratação e retificação.
	Infração normativa (há regra da empresa a respeito).	Advertência com aviso au superior hierárquico.
	Infração normativa com consequência para imagem da empresa ou reincidência.	Suspensão ou na reincidência desligamento.
	Infração de lei específica que já tipifica como ato ilícito (civil, adm, criminal).	Afastamento de cargo ou função ou desligamento.

INCIDENTES x RESPONSABILIDADE

LEVE	MÉDIO	GRAVE	GRAVÍSSIMO
			

Ato	Nível de gravidade
Compartilhar senha na rede	
Tentativa de acesso a site conteúdo pornográfico	
Portar conteúdo ou software pirata em notebook corporativo	
Tirar foto do ambiente da empresa e publicar na rede social	
Comentar rotina de trabalho na rede social	

INCIDENTES x RESPONSABILIDADE

LEVE	MÉDIO	GRAVE	GRAVÍSSIMO
			

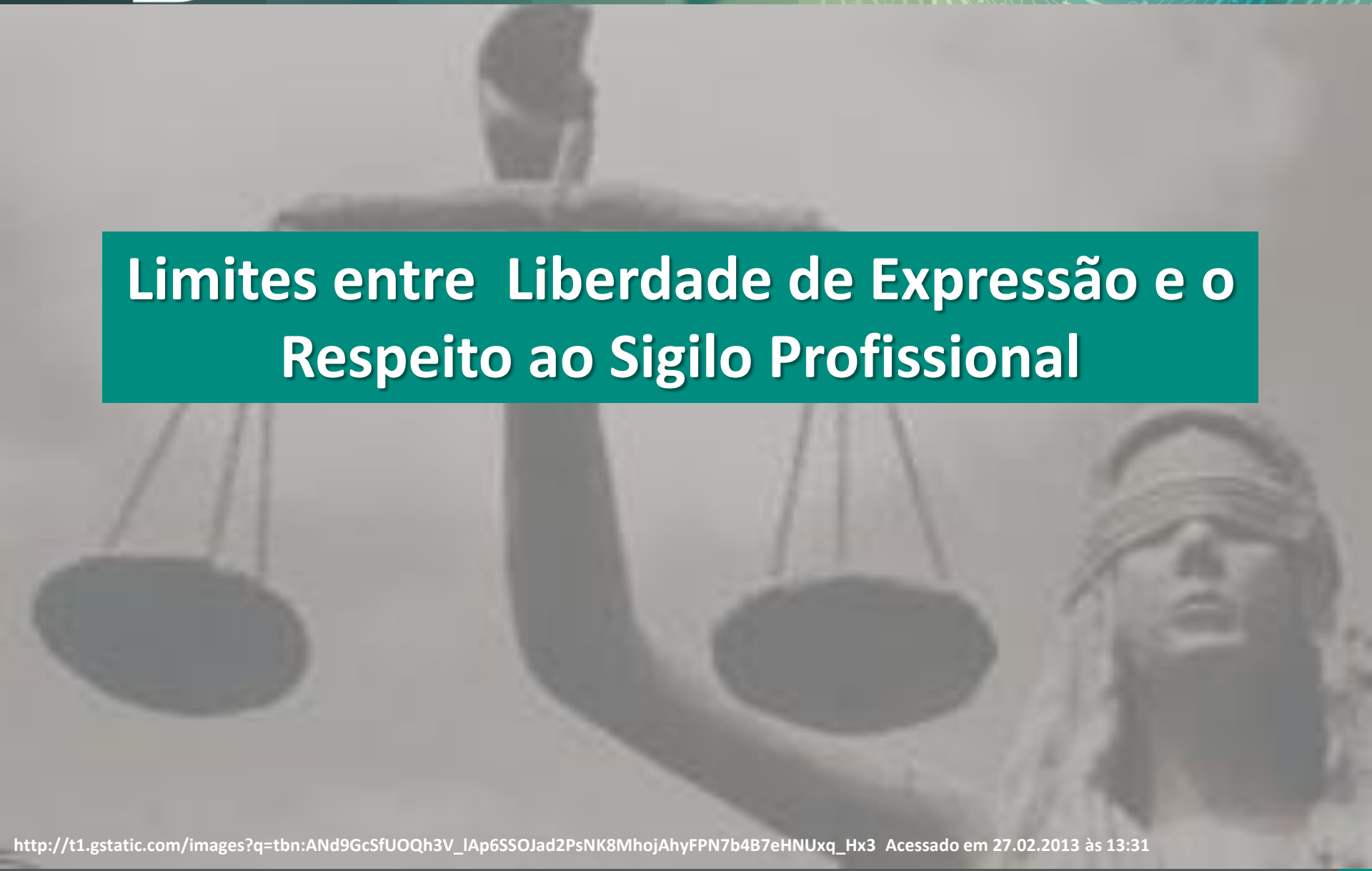
Compartilhar Senha da Rede	Nível de gravidade
Deixar equipamento sem bloqueio	
Enviar arquivo da rede para ex-funcionário	
Divulgar dados dos contribuintes a empresas de cobrança ou financeiras	
Portar, transmitir ou transportar dados sensíveis sem proteção	
Apagar dados usando credencial de colega que possui acessos privilegiados	

INCIDENTES x RESPONSABILIDADE

LEVE	MÉDIO	GRAVE	GRAVÍSSIMO
			

Compartilhar Senha da Rede	Nível de gravidade
Envio de e-mail para o destinatário errado	
Realizar o *download* de filmes e músicas via torrent na estação de trabalho	
Instalar um software não homologado pela empresa para aumentar a produtividade pessoal	
Encriptar dados com chave de propriedade pessoal	

Limites entre Liberdade de Expressão e o Respeito ao Sigilo Profissional



http://t1.gstatic.com/images?q=tbn:ANd9GcSfUOQh3V_lAp6SSOJad2PsNK8MhojAhyFPN7b4B7eHNUxq_Hx3 Acessado em 27.02.2013 às 13:31

Liberdade de Expressão X Sigilo Profissional

http://1.bp.blogspot.com/_gJ7Uyf3y_nQ/TQJKrh3vmZI/AAAAAAAAA_s/99Kkg2BOSRE/s1600/LIBERD%257E1.JPG Acessado em 27.02.2013 às 17:26.

Divulgação de Segredo

Código Penal, Art. 153 - Divulgar alguém, sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que é destinatário ou detentor, e cuja divulgação possa produzir dano a outrem:

Pena - detenção, de um a seis meses, ou multa.

§ 1º-A. Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública:

Pena - detenção, de 1 (um) a 4 (quatro) anos, e multa.

Violação de Segredo Profissional

Código Penal, Art. 154 - Revelar alguém, sem justa causa, segredo, de quem tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem.

Pena - detenção, de 3 (três) meses a 1 (um) ano, ou multa.

Código Civil

Art. 187 - Também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes.

Constituição Federal

Art. 5º - Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

IV - é livre a manifestação do pensamento, sendo vedado o anonimato.

PENAL E PROCESSUAL PENAL. RECURSO EM SENTIDO ESTRITO. DENÚNCIA IMPUTANDO A PRÁTICA DOS CRIMES DE PECULATO, DE CORRUPÇÃO PASSIVA E DE VIOLAÇÃO DE SIGILO FUNCIONAL. DENÚNCIA REJEITADA PARCIALMENTE, POR ENTENDER-SE NÃO CONFIGURADO O DELITO DE PECULATO, MAS APENAS O DE VIOLAÇÃO DE SIGILO. INOPORTUNIDADE DO JUÍZO. DECISÃO CASSADA

Trata-se de Recurso em Sentido Estrito interposto pelo Ministério Público para cassar a decisão do MM. Juiz de primeiro grau que rejeitou em parte a denúncia, aduzindo que "não houve o dolo dos denunciados para a prática do delito de peculato, pois nunca houve a intenção de apropriação de bem móvel da administração", pois, "ao que tudo indica até o momento, o que desejavam, desde o princípio, era a obtenção de dinheiro na venda do documento sigiloso" (f. 213).

O Tribunal entendeu que seria precipitado reconhecer a não configuração ou a absorção de crimes durante o curso do processo, ainda mais por ocasião do recebimento da denúncia.

Ante o exposto, foi dado provimento ao recurso do Ministério Público Federal **para cassar a decisão de rejeição parcial da denúncia, determinando o prosseguimento do feito em primeiro grau de jurisdição, sem decotes na acusação formulada e, por outro lado, sem prejuízo de futura desclassificação das condutas.**

RECURSO EM SENTIDO ESTRITO Nº 0001779-03.2010.4.03.6181/SP – Tribunal Regional Federal da 3ª Região – 06/05/2011

Um dos LIMITES da Liberdade de Expressão é o Sigilo Profissional, além dos direitos relativos à imagem, à honra, à reputação e os relacionados à autoria

Lei nº 6.123 de 20 de julho de 1968
Art. 194. Ao funcionário público é proibido:
III - Retirar, sem previa autorização da autoridade competente, qualquer documento ou objeto da repartição

http://bebegravidez.com/wp-content/uploads/2011/09/Limites-sejam-impostos-%C3%A0s-crian%C3%A7as.jpg Acessado em 27.02.2013 às 17:48.

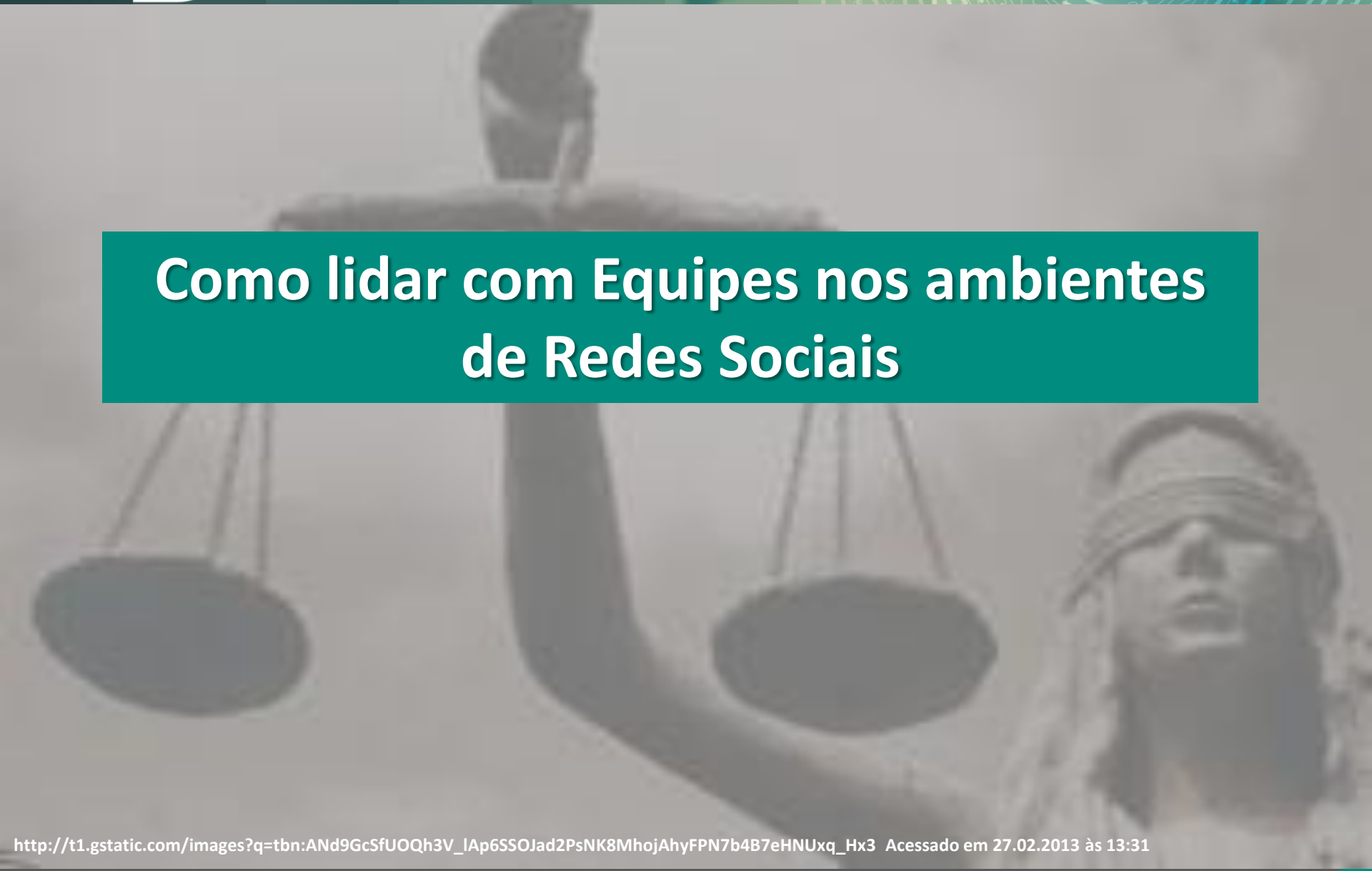
Política de Segurança da Informação

Art. 20, Parágrafo único - Todos os ativos e informações do TJPE devem ser utilizados apenas para o cumprimento das atividades profissionais dentro do padrão de conduta ética estabelecida pela Estrutura Normativa de Segurança da Informação do TJPE e às demais leis em vigor, respeitando os requisitos de sigilo profissional.

Norma para Classificação da Informação

5.1.6. Todos os agentes judiciários e demais colaboradores têm o dever de assegurar a proteção das informações, dados ou documentos que tiverem contato contra perda, acesso, alteração, transmissão e divulgação não autorizados ou indevidos. Aquele que obtém acesso à informação, dado ou documento do TJPE é obrigado a manter seu sigilo de acordo com a classificação imposta

Como lidar com Equipes nos ambientes de Redes Sociais



http://t1.gstatic.com/images?q=tbn:ANd9GcSfUOQh3V_lAp6SSOJad2PsNK8MhojAhyFPN7b4B7eHNUxq_Hx3 Acessado em 27.02.2013 às 13:31

A Administração Pública está nas redes sociais

Portaria n.º 38 do Conselho da Defesa Nacional

Norma Complementar nº 15/IN01/DSIC/GSIPR

http://redessociais.me/wp-content/uploads/2012/08/monitoramento.png Acessado em 28.02.2013 às 16:42.

Lidar com Equipes

STF

@STF_oficial Brasília - DF

O STF é o órgão de cúpula do Poder Judiciário, e a ele compete, precipuamente, a guarda da Constituição, conforme definido no art. 102 da Constituição Federal.

http://www.stf.jus.br

STF_oficial STF
Ouvi por aí: "agora que o Ronaldo se aposentou, quando será que o Sarney vai resolver pendurar as chuteiras?"
25 minutes ago Favorite Retweet Reply

http://www1.folha.uol.com.br/poder/875853-twitter-do-stf-pergunta-quando-sarney-vai-pendurar-chuteiras.shtml acessado em 19.2.2013 às 20h09

CUIDADO: As Redes Sociais precisam ser utilizadas com cautela.

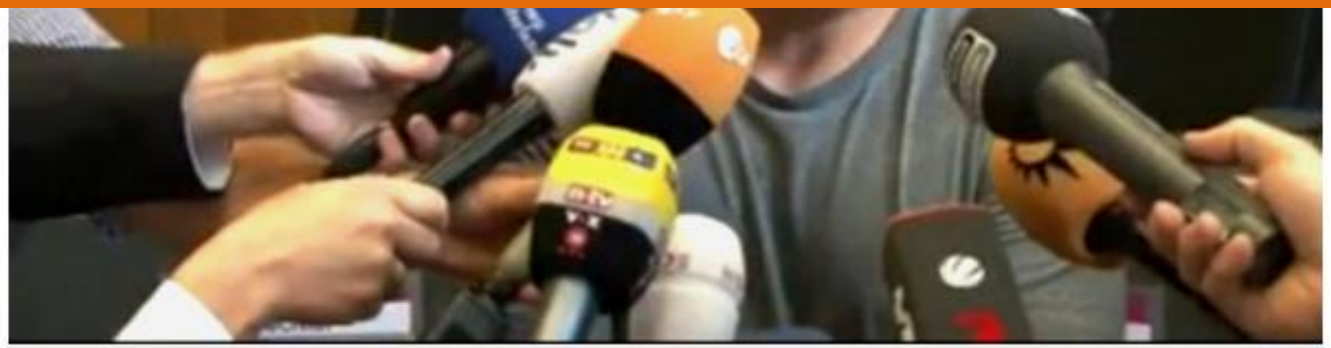
msn
facebook
flickr
orkut beta
Google+

http://img1.mlstatic.com/placa-pet-perigo-cuidado-comercio-industria-epi_MLB-O-104019536_7478.jpg e http://3.bp.blogspot.com/-6RtmMQ_vq5s/UP581NRTPkI/AAAAAAAABZ4/z1oAfUOOsWE/s1600/aba.png Acessado em 28.02.2013 às 10:09.

'Assassinato do Facebook': garoto de 15 anos é condenado

Discussão na rede social teria levado casal de namorados a contratar garoto para matar adolescente. Mandantes serão julgados no próximo mês

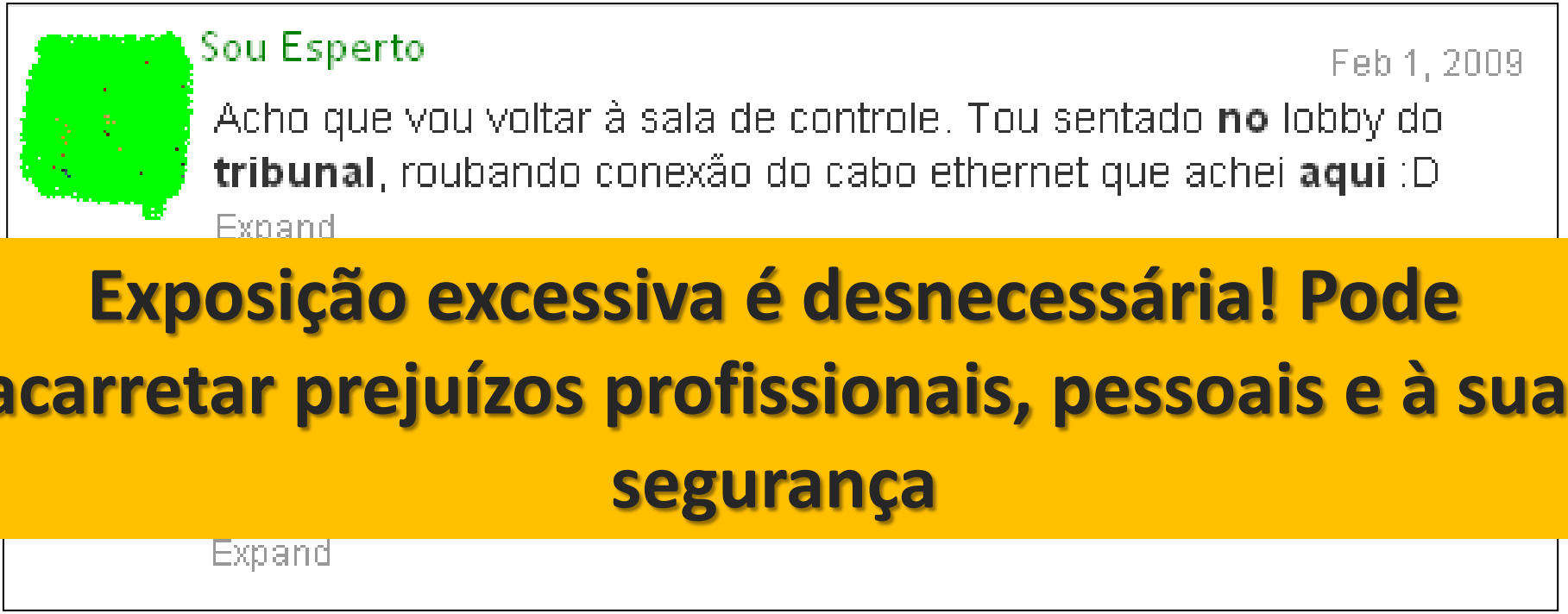
Não tenha discussões profissionais nas redes sociais!



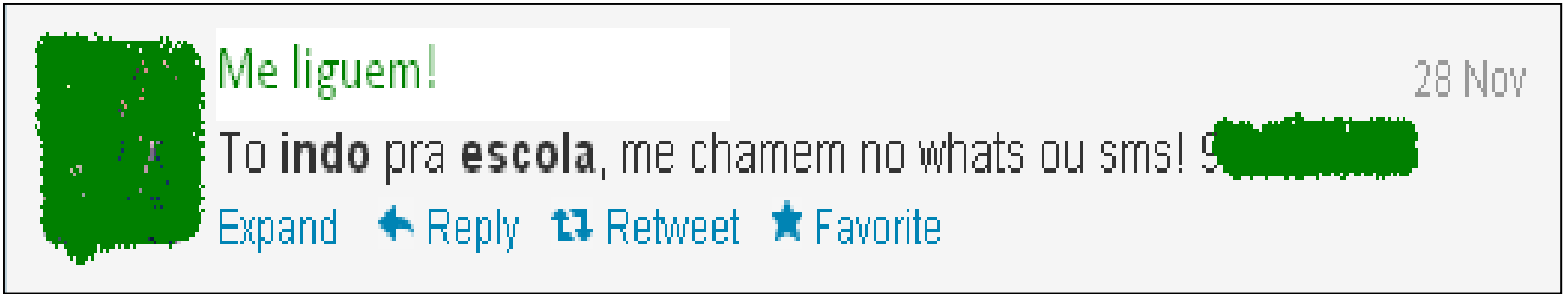
O pai de Winsie, Chun Nam Hau (Reprodução de TV)

Um garoto holandês de 15 anos de idade foi condenado nesta segunda-feira a um ano de detenção em um reformatório, além de ter que passar outros três anos em uma instituição psiquiátrica, após confessar ter esfaqueado até a morte uma adolescente de 15 anos. O caso

http://veja.abril.com.br/noticia/internacional/jov
esfaquear-uma-garota Acessado em 28.02.2013 à
do-na-holanda-apos-



Exposição excessiva é desnecessária! Pode acarretar prejuízos profissionais, pessoais e à sua segurança



Como lidar com o uso das redes sociais pela sua Equipe?

http://2.bp.blogspot.com/_U2e8azn9Bwo/SOzR7dmGL9I/AAAAAAAAAm8/Lo7nQ4-QBLc/s320/cabelo_em_pe.jpg Acessado em 28.02.2013 às 10:45.

Lidar com Equipes

- Oriente e estimule o uso ético, seguro e legal das Redes Sociais;
- Recomende que sua equipe tenha uma postura adequada no uso destes ambientes eletrônicos e em hipótese alguma façam uso dos mesmos para prática de ofensas, atos ilícitos ou antiéticos;
- Informe que eles não devem fazer qualquer referência ou uso da marca ou nome da instituição, sem prévia autorização desta;
- Libere o acesso institucional apenas se estiver atrelado a atividade profissional desenvolvida;
- Isso deve estar claro no Código de Ética e na Norma específica para Redes Sociais.

ESTUDO DE CASO

Ao acessar o perfil de um agente judiciário no facebook você percebe que lá foram divulgadas informações sigilosas de sua área. O que você faz?

Resposta: Dar ciência ao responsável pela Segurança da Informação ou Gestão de Incidentes da instituição.

http://macaibaindependente.com.br/wp-content/uploads/2012/12/livros-estudo.jpg Acessado em 15.02.2013 às 15:36.

E o que o Tribunal poderá fazer?

✓ Lavrar Ata Notarial para preservação da prova ou Print Screen da tela;

✓ Solicitar ao titular do perfil a remoção do conteúdo (solução amigável);

✓ Notificar legalmente o controlador da rede social para exclusão do conteúdo;

✓ Investigar a autoria do fato internamente e se comprovada a culpa ou dolo, iniciar processo administrativo competente;

✓Não surtindo efeito, ajuíza-se Ação de Obrigação de Fazer com Pedido de Tutela Antecipada contra a rede social para obter a referida exclusão.

http://t0.gstatic.com/images?q=tbn:ANd9GcSSTLwZN-9NDxus2WZrQlwgUm8pCFwZZJg55EfGaMBWFG3TdWpQaA Acessado em 15.02.2013 às 15:43.

Portaria nº 38 de 2012 - CONSELHO DE DEFESA NACIONAL

Definiu boas práticas para a utilização dos canais de mídias sociais por órgãos da Administração Pública Federal, que podem ser aproveitadas pelo TJPE, da seguinte forma:

1. Definir quem será o Administrador de Perfil e o Agente Responsável;
2. Fazer o registro dos perfis oficiais nas Redes Sociais (em especial no Facebook, Twitter e Linkedin);
3. Implementar ferramenta de Monitoramento específico das Redes Sociais (que possa identificar as interações dos perfis oficiais e também o que ocorre fora deles);

Portaria nº 38 de 2012 - CONSELHO DE DEFESA NACIONAL

4. Elaborar o plano de resposta a incidentes e a crise de imagem digital (já prevendo ações, SLAs, registro e coleta de provas legais, modelo de instauração de processo administrativo ou judicial se necessário, respostas rápidas);
5. Capacitar a equipe interna ou a equipe mista que fará a gestão dos perfis oficiais bem como a análise dos relatórios de monitoramento;
6. Elaborar e implementar o Termo de Responsabilidade para assinatura dos usuários;
7. Elaborar o Manual de Postura Ética e Segura do Agente Judiciário na Rede Social;

Portaria nº 38 de 2012 - CONSELHO DE DEFESA NACIONAL

8. Realizar a Campanha de Conscientização para os usuários específica sobre o tema das Redes Sociais;
9. Realizar reunião periódica do Comitê de Segurança da Informação e Comunicações para análise de riscos em Redes Sociais, planejamento de ações e implementação de medidas (é recomendável que se reúna no máximo em intervalos de até 3 meses);
10. Fazer uso de empresas e consultores especialistas em Redes Sociais, Direito Digital, Segurança da Informação para gerar conhecimento e treinar os times internos, bem como apoiar na geração e revisão de toda a documentação.

Monitoramento Corporativo X Privacidade

http://t1.gstatic.com/images?q=tbn:ANd9GcSfUOQh3V_lAp6SSOJad2PsNK8MhojAhyFPN7b4B7eHNUxq_Hx3 Acessado em 27.02.2013 às 13:31

PRIVACIDADE é um direito MULTIFACETADO!

- ✓ Proteção de Imagem e Reputação
- ✓ Proteção de vida privada
- ✓ Proteção de intimidade (partes físicas do corpo)
- ✓ Proteção de Dados Pessoais
- ✓ Proteção do Domicílio
- ✓ Proteção de Informação (transmissão de comunicação, correspondência)

Pode haver o monitoramento das informações e dos ambientes físicos e lógicos do Tribunal?

SIM, desde que....

Haja o aviso prévio, visível e objetivo do monitoramento
e
Obrigação expressa do uso do recurso institucional apenas para finalidade profissional.

LEGALIDADE DE MONITORAMENTO DE E-MAIL CORPORATIVO. DESLIGAMENTO POR MAU PROCEDIMENTO.

Desse modo, tendo em conta o teor do conjunto probatório produzido no feito, outra conclusão não se pode admitir senão a **de que o reclamante, de fato, enviou e/ou repassou as mensagens de conteúdo pornográfico**, até mesmo porque não há nos autos qualquer indício contundente de que outro empregado tenha se aproveitado de momentos de ausência do autor para utilizar indevidamente o equipamento e conta de e-mail deste para fins de divulgação de material pornográfico.

No caso do 'e-mail corporativo', todavia, essa forma de comunicação vai além de um mero serviço postal ou depósito de mensagens, mas **configura autêntico instrumento de comunicação virtual disponibilizado pelo empregador, equiparando-se, pois, a uma ferramenta de trabalho.**

Portanto, esse meio de comunicação **destina-se essencialmente à troca de mensagens de caráter profissional.**

PROCESSO Nº TST-AIRR-159700-03.2008.5.15.0062. Ministro Relator JOSÉ ROBERTO FREIRE PIMENTA. Brasília 29/02/2012

E como estão as Normas internas do Tribunal?

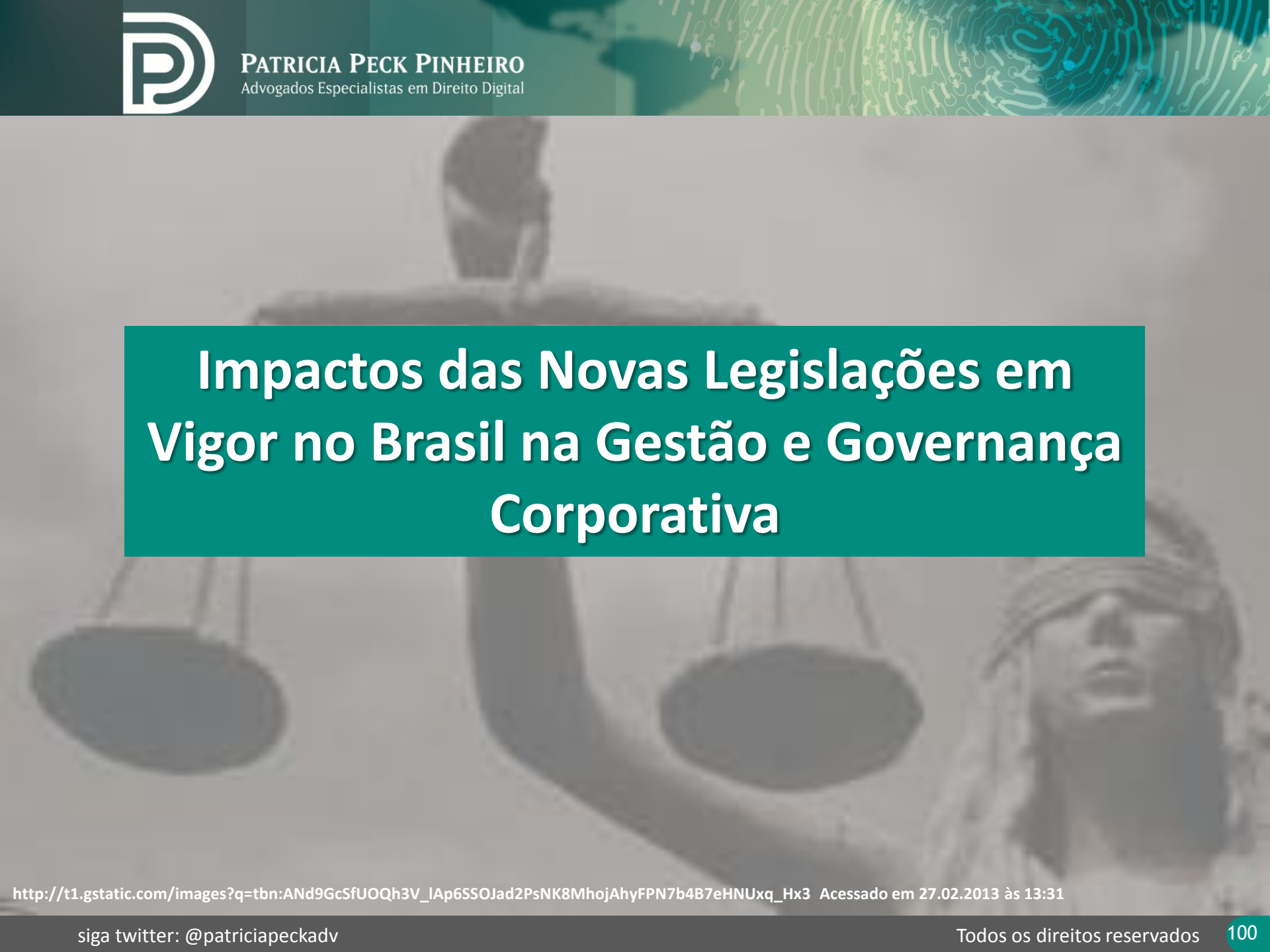
http://www.globalframe.com.br/gf_base/empresas/MIGA/imagens/781606FD1C6665F1279EC61CCEC7D3A7B996_normas.jpg Acessado em 25.02.2013 às 14:57.

Norma de Utilização de Ativos de Informação e Recursos de Tecnologia da Informação e Comunicação

5.1.1. Os recursos de TIC são destinados para finalidades estritamente profissionais e restritas às atividades designadas para cada agente judiciário e colaboradores.

5.7.1. Os agentes judiciários e colaboradores estão cientes de que o TJPE monitora todo acesso e uso de suas informações, marcas e recursos de TIC, além de seus ambientes físicos e/ou lógicos com a finalidade de proteção de seu patrimônio, reputação e daqueles com quem se relaciona, através da captura de imagens, áudio e vídeo, inclusive, realizando o armazenamento dos dados monitorados para fins administrativos e legais.

Impactos das Novas Legislações em Vigor no Brasil na Gestão e Governança Corporativa



http://t1.gstatic.com/images?q=tbn:ANd9GcSfUOQh3V_lAp6SSOJad2PsNK8MhojAhyFPN7b4B7eHNUxq_Hx3 Acessado em 27.02.2013 às 13:31

Lei de Crimes Eletrônicos

http://www.femipa.org.br/blog/wp-content/uploads/legisla%C3%A7%C3%A3o.jpg Acessado em 28.02.2013 às 16:50.

Caso: Carolina Dieckmann

Links matérias: http://g1.globo.com/globo-news/noticia/2012/05/computador-nao-deve-ter-dados-comprometedores-alerta-especialista-em-direito-de-internet.html e http://g1.globo.com/bom-dia-brasil/noticia/2012/05/especialistas-dao-dicas-sobre-como-manter-privacidade-no -mundo-digital.html

Fonte : Carolina Dieckmann - http://bit.ly/KFA5oN

Coleta ≠ Publicação ≠ Contexto

Depois que uma imagem está na internet ela pode ser replicada inúmeras vezes!

http://www.twilk.com.br/wp-content/uploads/2011/08/mosaico-twilk-300x188.jpg Acessado em 27.08.2012 às 17:38.

Lei nº 12.737, de 30 de novembro de 2012

Invasão de dispositivo informático:

Art. 154-A: Invadir dispositivo informático alheio, conectado ou não a rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades:

Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa.

Lei nº 12.737, de 30 de novembro de 2012

§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.

§ 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.

§ 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:

Pena – reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.

Lei nº 12.737, de 30 de novembro de 2012

Invasão de dispositivo informático

Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.

Lei nº 12.737, de 30 de novembro de 2012

Art. 266. Art. 266 - Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento:

Pena - detenção, de um a três anos, e multa.

§ 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.

§ 2º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública.

Lei nº 12.737, de 30 de novembro de 2012

Pontos faltantes da lei:

- ✓ **Crimes de DDoS contra pessoas jurídicas de direito privado, não somente públicas (ou em função pública);**
- ✓ **Criação e Disseminação de vírus, bombas lógicas, cavalos de tróia ou demais programas maliciosos;**
- ✓ **A quebra de segurança pura ou esforços seguidos que constituem a tentativa;**
- ✓ **Mascaramento de conexões ou desvio de rotas de pacotes de rede.**

Lei de Acesso à Informação

http://www.femipa.org.br/blog/wp-content/uploads/legisla%C3%A7%C3%A3o.jpg Acessado em 28.02.2013 às 16:50.

Lei 12.527/2011

Lei de Acesso à Informação
Entrou em vigor dia 16/maio/2012

Respeite os rótulos de Sigilo das informações!
Ultrassecreta, Secreta, Reservada, Confidencial, Interna e Pública

divulgação.

Mas também a portaria **elenca os documentos considerados sigilosos** para garantir a segurança da sociedade e a sua imprescritibilidade.

Nova Legislação

Veja abaixo os contracheques divulgados pela ministra Cármen Lúcia.

PODER JUDICIÁRIO
SUPREMO TRIBUNAL FEDERAL
CNPJ: 00.531.640/0001-28

Demonstrativo de Pagamento

Matrícula	Nome do Servidor	Situação
50	CÁRMEN LÚCIA ANTUNES ROCHA	MINISTRO

Lotação	Data de Exercício
STF - MIN - GABINETE MINISTRA CÁRMEN LÚCIA	21/06/2006
Cargo Efetivo	**Nível-Classe-Padrão**
MINISTRO	VMINIS
Código / Nível / **Cargo em Comissão / Função Gratificada**	**CPF**
	254.860.806-97

Banco	Agência	C.Corrente	Anuênio	Quinquênio	Dep SF	Dep IR	Mês/Ano
1	48852	151386	0		0	0	MAI/2012

Código	Tipo	Discriminação	Parcela	Qtd.	Créditos - R$	Débitos - R$
0008	R	SUBSÍDIO	F	1	26.723,13	
6001	D	PSSS	1	1		2.939,54
6010	D	IR	1	1		5.783,96
6401	D	STF-MED CONTRIBUIÇÃO	1	1		122,14

Previsão de Crédito	Margem Consignável - R$	Bruto - R$	Descontos - R$	Líquido - R$
22/05/2012	R$ 7.894,80	R$ 26.723,13	R$ 8.845,64	R$ 17.877,49

Mensagem:

http://g1.globo.com/politica/noticia/2012/05/presidente-do-tse-divulga-contracheques-no-site-do-tribunal.html

Lei 12.257/2011 – Lei de Acesso a Informação

✓Visa assegurar o direito fundamental de acesso à informação, (princípio da publicidade - art. 3º inc I).

✓ As informações protegidas pela legislação devem ser classificadas em ultrassecreta, secreta e reservada com prazos máximos de restrição de acesso de **25, 15 e 5 anos**, respectivamente (art. 23 e 24 – segredo de justiça ou segredo industrial Lei 9279/96, segurança nacional).

✓ Transcorrido este prazo a informação será automaticamente desclassificada para pública.

✓Haverá casos específicos de tratamento de informações pessoais tratada em capítulo específico da Lei, onde deverá ter, como regra geral, a garantia a privacidade das informações pessoais.

Decreto nº 7.724, de 16 de maio de 2012

Art. 1º - Este Decreto regulamenta, no âmbito do Poder Executivo Federal, os procedimentos para a garantia do acesso à informação e para a classificação de informações sob restrição de acesso, observados grau e prazo de sigilo, conforme o disposto na Lei no 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5o, no inciso II do § 3o do art. 37 e no § 2o do art. 216 da Constituição.

Lei Estadual de Pernambuco nº 14.804, de 29 de outubro de 2012.

Regula o acesso a informações, no âmbito do Poder Executivo Estadual, e dá outras providências.

Art. 1º - Art. 1º Fica garantido o direito fundamental de acesso às informações, no âmbito do Poder Executivo Estadual, consoante normas gerais disciplinadas na Lei Federal nº 12.527, de 18 de novembro de 2011.

Decreto/PE nº 38.787, de 30 de outubro de 2012

Art. 1º - Art. 1º Este Decreto regulamenta, no âmbito do Poder Executivo Estadual, os procedimentos para a garantia do acesso à informação e para a classificação de informações sob restrição de acesso, observados grau e prazo de sigilo, conforme o disposto na Lei no 14.804, de 29 de outubro de 2012, que regula o acesso a informações, previsto no inciso XXXIII do caput do artigo 50, no inciso II do § 30 do artigo 37 e no § 20 do artigo 216, todos da Constituição Federal, no âmbito do Poder Executivo Estadual.

Decreto 7.845/2012 (desde novembro)

CIDIC – Código de Indexação de Documento que contém Informação Classificada

✓Os órgãos ou entidades são obrigados a proteger as informações sigilosas sob sua custódia contra qualquer uso ou acesso indevido;

✓O CIDIC é composto por um número único de protocolo e pelos seguintes elementos: grau de sigilo, categoria, data de produção da informação, data da desclassificação da informação classificada, indicação da reclassificação e da data de prorrogação da manutenção da classificação. Deverá ser mantido todo o histórico de alterações;

Decreto 7.845/2012 (desde novembro)

CIDIC – Código de Indexação de Documento que contém Informação Classificada

✓Após a classificação, a informação só poderá ser tratada por órgão ou entidade detentor de credencial de segurança fornecida por órgão habilitado pelo Núcleo de Segurança e Credenciamento - instituído no âmbito do Gabinete de Segurança Institucional da Presidência da República;

✓Credencial de segurança é o certificado que autoriza pessoa para o tratamento da informação classificada.

Principais pontos alterados nos Normativos do Tribunal de Justiça

http://t1.gstatic.com/images?q=tbn:ANd9GcSfUOQh3V_lAp6SSOJad2PsNK8MhojAhyFPN7b4B7eHNUxq_Hx3 Acessado em 27.02.2013 às 13:31

Por que devemos realizar a blindagem legal da Política de Segurança da Informação?

- Para atender requisito de governança corporativa;
- Para atender indicador de auditoria;
- Para estar em conformidade com ISOs (27001, 27002);
- Para gerar prevenção e servir de diretriz comportamental (evitar incidentes);
- Para evitar interpretação pessoal que pode responsabilizar o gestor (alegação de perseguição, discriminação, invasão de privacidade);
- Para gerar proteção jurídica e que o documento possa ser usado se necessário para punir infrator e para defesa no judiciário.

O que deve conter a Política de Segurança de Informação

- ✓ Propriedade da Informação e dos Recursos Corporativos.
- ✓ Dever proteção da identidade digital e de uso de padrão de senha segura.
- ✓ Dever proteção dos ativos intangíveis de reputação e conhecimento.
- ✓ Obrigatoriedade do uso dos recursos corporativos para finalidade profissional limitada a alçada e função.
- ✓ Dever de cumprir com sigilo profissional.
- ✓ Dever de confidencialidade e de uso de cláusulas de confidencialidade e assinatura de NDAs.
- ✓ Dever de uso de cláusulas de segurança da informação em contratos de trabalho e de terceirizados.
- ✓ Dever de backup.
- ✓ Dever de classificação da informação.

O que deve conter a Política de Segurança de Informação

- ✓ Dever de cumprir com o nível de segurança exigido pela classificação.
- ✓ Dever de descarte seguro.
- ✓ Dever de mesa limpa.
- ✓ Dever de uso de conteúdos legais e legítimos.
- ✓ Proibição de conteúdos pessoais, pornográficos, ilícitos.
- ✓ Proibição de coleta de fotos e imagens no perímetro físico da empresa bem como de sua publicação sem autorização prévia da empresa.
- ✓ Aviso claro e objetivo de Inspeção Física (alcançando também dispositivos particulares dentro do perímetro físico).
- ✓ Aviso claro e objetivo de Monitoramento irrestrito (alcançando também dispositivos particulares dentro do perímetro físico e lógico).

O que deve conter a Política de Segurança de Informação

- ✓ Dever de mobilidade segura independente de quem fornece o dispositivo (conforme nova regra do art. 6º. da CLT), bastando que seja informação da empresa (inclui uso de bloqueio de acesso (seja celular, pendrive, notebook ou tablet), dever de criptografia, dever de backup, vedação para envio de conteúdo corporativo para caixa postal de e-mail particular, vedação de uso de pastas de compartilhamento gratuito de arquivos de forma pública como Dropbox e Slideshare), vedação para uso de 3G e navegação em paralelo (fora do firewall) se não tiver sido autorizado, orientação sobre uso de rede wi-fi.
- ✓ Orientação sobre o acesso seguro ao invés de portar dados (deve portar sempre menor quantidade possível pelo menor tempo, apenas o estritamente necessário e sempre em dispositivo com bloqueio de acesso).

O que deve conter a Política de Segurança de Informação

- ✓ Aviso que o mero acesso ao recurso pode ocorrer de forma remota e a qualquer horário e, por si só, não configura sobrejornada nem hora extra.
- ✓ Orientação sobre postura em Redes Sociais (independente do tipo de conexão e do tipo de perfil, se corporativo ou pessoal), tratando sobre uso de marca, informações de rotina de trabalho, tratamento respeitoso e ético com os colegas.
- ✓ Dever de denúncia imediata de incidente.
- ✓ Responsabilidade do gestor sobre os recursos e postura de sua equipe.
- ✓ Aviso de que a tentativa de burlar será considerada também infração.
- ✓ Informação de que a empresa irá colaborar com as autoridades.
- ✓ Dever de Educação e Conscientização.
- ✓ Dever de guarda das provas.

O que deve conter a Política de Segurança de Informação

- ✓ Dever de observar questões de segurança da informação no processo de seleção de pessoas.
- ✓ Aviso de penalidades.
- ✓ Obrigação de formação e atuação do Comitê de Segurança da Informação.
- ✓ Informação onde encontrar os documentos de Segurança da Informação.
- ✓ Dever do colaborador se manter sempre atualizado e ciente das normas da empresa.
- ✓ Obrigatoriedade de uso de recursos de segurança (antivírus, firewall).
- ✓ Glossário de Termos técnicos.
- ✓ Dever de atualização periódica do documento (em intervalo não superior a 2 anos).
- ✓ Recomendações para proteção contra Engenharia Social.

Judiciário decide a Favor

CASO: Não observância as regras da empresa, uso indevido das ferramentas de trabalho (computador e internet).

"RITO SUMARÍSSIMO. RECURSO ORDINÁRIO. JUSTA CAUSA. ART. 482, "b", DA CLT. **Burla de regras da empresa para acesso a sítios, o que era vedado.** Norma regulamentar da qual o reclamante tinha conhecimento prévio. **Computador e internet, instrumentos de trabalho utilizados irregularmente, para uso pessoal. Incontinência de conduta e mau procedimento. Falta grave que está caracterizada.**"

(TRT02, RO 01875200843102004, Relator Carlos Francisco Berardo, Julgado em 17/02/2009).

Alteração dos Normativos

O que é juridicamente recomendável, ou não, para a Segurança da Informação:

Não Recomendável	Recomendável
Presunção ou faculdade de monitoramento	Monitoramento efetivo
Monitorar sem avisar previamente ou Monitorar dizendo que é eventual (sem a certeza de sua ocorrência dando margem a dúvida)	Aviso de monitoramento prévio, visível e objetivo não apenas na política, mas também com inserção de cláusula em contratos de trabalho, contratos de terceirizados, nas interfaces gráficas, no aviso legal do rodapé de email
Linguagem genérica, ineficaz e incoerente a exemplo de “consciente” e “racional”	Linguagem direta, objetiva e eficaz a exemplo de “adequado” e “correto”

Alteração dos Normativos

O que é juridicamente recomendável, ou não, para a Segurança da Informação:

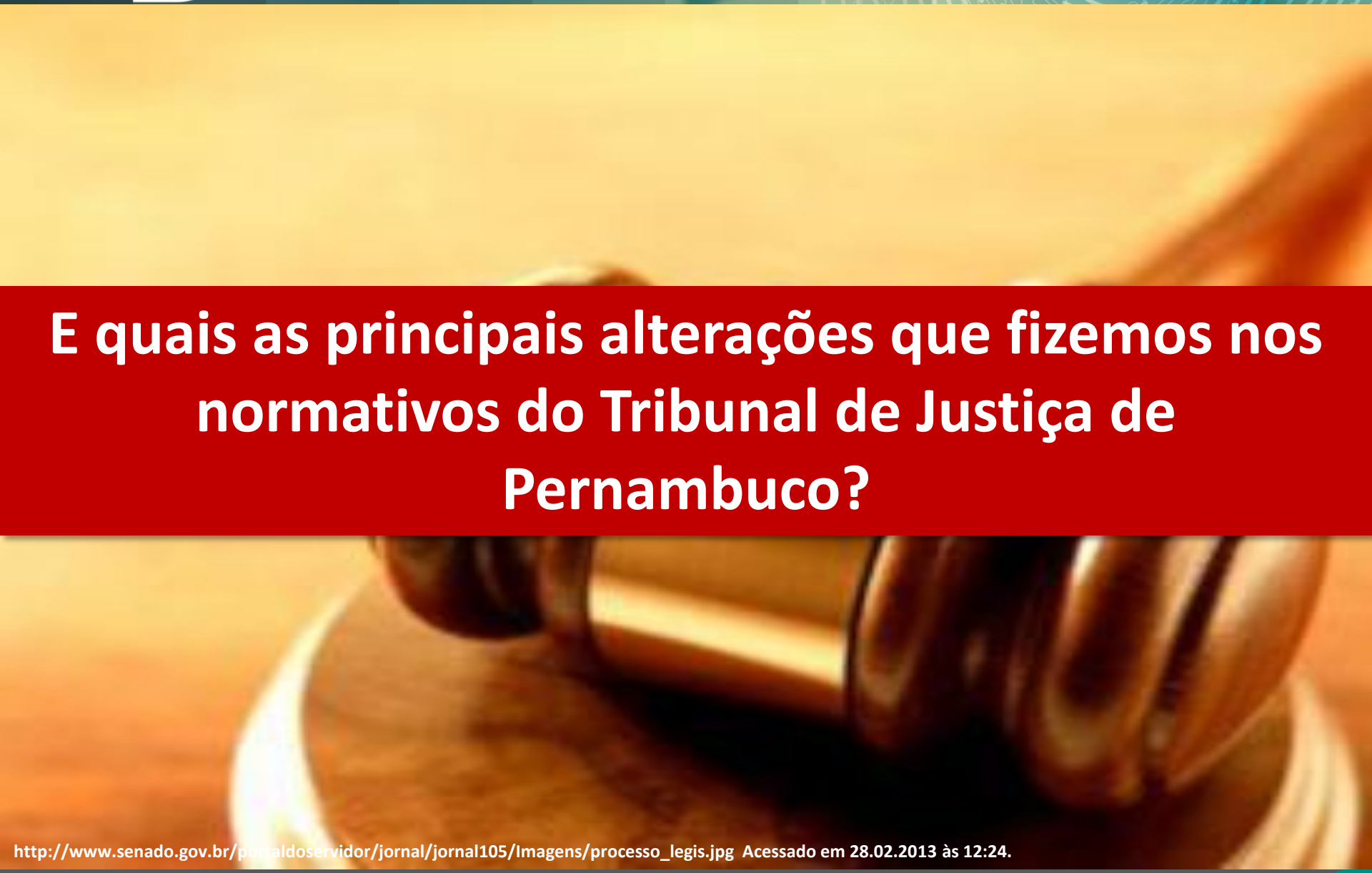
Não Recomendável	Recomendável
Solicitar o *login* e senha do colaborador para verificar suas atividades em serviços que acessa na internet (ex. mídias sociais)	Orientar o colaborador para o uso ético, seguro e legal dos serviços que acessa na internet
Foco em punições quando houver o descumprimento de normas	Estimular o cumprimento das normas com bonificações ou permissões a recursos benéficos ao cotidiano profissional do colaborador
Normas com condão repressivo	Normas com condão preventivo, educativo e comportamental

Alteração dos Normativos

O que é juridicamente recomendável, ou não, para a Segurança da Informação:

Não Recomendável	Recomendável
Punições ridicularizantes ou exposição indevida de certos conteúdos interceptados	Agir sempre com discrição e proporcionalidade. A punição possui efeito pedagógico perante os demais mesmo quando não expõe o transgressor

E quais as principais alterações que fizemos nos normativos do Tribunal de Justiça de Pernambuco?



http://www.senado.gov.br/portaldoservidor/jornal/jornal105/Imagens/processo_legis.jpg Acessado em 28.02.2013 às 12:24.

Alteração dos Normativos

Indicador	Nova Cláusula
Propriedade da Informação e dos Recursos Corporativos.	**Art. 20 da PSI -** Todas as informações criadas, acessadas, compartilhadas, manuseadas, armazenadas ou disponibilizadas ao agente judiciário ou das quais tiver acesso no exercício de suas atividades, são de propriedade e/ou direito de uso exclusivo do TJPE.
Dever proteção da identidade digital e de uso de padrão de senha segura.	**Art. 18 da PSI -** O agente judiciário deve proteger sua identidade digital, devendo suas credenciais, senhas e acessos ser pessoais e tratadas de forma segura, confidencial, intransferível, intransmissível e possuir apenas as permissões suficientes para realização das suas atividades com orientação nos princípios do conjunto mínimo de permissões que precisam ser atribuídos (least privilege e need to know). 5.5.4. da Norma de Controle de Acesso - As senhas aplicadas nos ativos de informação ou recursos de TIC do TJPE devem ter no mínimo 8 (oito) caracteres alfanuméricos e conterem pelo menos uma letra maiúscula, uma letra minúscula e um número.

Alteração dos Normativos

Indicador	Nova Cláusula
Dever proteção dos ativos intangíveis de reputação e conhecimento.	**Art. 25 da PSI -** Este Poder monitora todos os recursos, ambientes, dispositivos e ativos ligados à Tecnologia de Informação e Comunicação, tais como, mas não se restringindo ao e-mail institucional, acesso à internet, estrutura de comunicação telefônica, espaços físicos e utilização dos dispositivos de TIC institucionais, com a finalidade de proteger seus ativos, sua reputação e conhecimento.
Obrigatoriedade do uso dos recursos corporativos para finalidade profissional limitada a alçada e função.	**Art. 20, Parágrafo único da PSI -** Todos os ativos e informações do TJPE devem ser utilizados apenas para o cumprimento das atividades profissionais dentro do padrão de conduta ética estabelecida pela Estrutura Normativa de Segurança da Informação do TJPE e às demais leis em vigor, respeitando os requisitos de sigilo profissional.

Alteração dos Normativos

Indicador	Nova Cláusula
Dever de cumprir com sigilo profissional.	**Art. 20, Parágrafo único da PSI -** Todos os ativos e informações do TJPE devem ser utilizados apenas para o cumprimento das atividades profissionais dentro do padrão de conduta ética estabelecida pela Estrutura Normativa de Segurança da Informação do TJPE e às demais leis em vigor, respeitando os requisitos de sigilo profissional.
Dever de confidencialidade e de uso de cláusulas de confidencialidade e assinatura de NDAs.	**Art. 36 da PSI -** Todos os relacionamentos e contratações em que haja o compartilhamento de informações ou ativos de TIC deste Poder ou a concessão de qualquer tipo de acesso aos seus ambientes e recursos devem ser precedidos por Termos de Confidencialidade e cláusulas contratuais que tratem especificamente da Segurança da Informação. **Art. 7º, I da PSI –** Cabe aos agentes judiciários firmar, obrigatoriamente, Termo de Responsabilidade e Confidencialidade sobre as informações.

Alteração dos Normativos

Indicador	Nova Cláusula
Dever de uso de cláusulas de segurança da informação em contratos de trabalho e de terceirizados.	**Art. 36 da PSI -** Todos os relacionamentos e contratações em que haja o compartilhamento de informações ou ativos de TIC deste Poder ou a concessão de qualquer tipo de acesso aos seus ambientes e recursos devem ser precedidos por Termos de Confidencialidade e cláusulas contratuais que tratem especificamente da Segurança da Informação. **Art. 7º, I da PSI –** Cabe aos agentes judiciários firmar, obrigatoriamente, Termo de Responsabilidade e Confidencialidade sobre as informações.
Dever de backup.	**5.11.2 da Norma para Disp. Mobilidade -** Todos agentes judiciários e demais colaboradores que fizerem uso dos dispositivos de mobilidade devem realizar cópia de segurança (backup) das informações diária ou por intervalo máximo semanal, com procedimento a ser definido pela SETIC, além de manterem os softwares de segurança da informação exigidos para a proteção e o uso seguro do equipamento e das informações sempre ativos e atualizados.

Alteração dos Normativos

Indicador	Nova Cláusula
Dever de classificação da informação.	**Art. 15 da PSI -** Cabe aos responsáveis pela informação a sua classificação e a definição de quem possui acesso e seu tipo de privilégios de acesso, sem prejuízo do disposto na legislação vigente.
Dever de cumprir com o nível de segurança exigido pela classificação.	**Art. 16 da PSI -** Os agentes judiciários tem o dever de cumprir com o nível de segurança exigido pela classificação das informações, sob pena de interposição de Processo Administrativo que poderá restar em sanção severa conforme a gravidade do ato e os prejuízos sofridos.
Dever de descarte seguro.	**Art. 37 da PSI -** O descarte de informações e ativos de TIC do TJPE devem ser realizados de forma segura, com a destruição, sanitização ou inutilização da mídia ou dispositivo que contém as informações, de modo que fique incapacitada de ser recuperada, adquirida ou reutilizada por terceiros.

Alteração dos Normativos

Indicador	Nova Cláusula
Dever de uso de conteúdos legais e legítimos.	**Art. 27 da PSI -** É vetado aos agentes do judiciário acessar ou armazenar, a partir de dispositivos ou recursos de TIC do TJPE ou pessoais em seu proveito, conteúdo que caracterize atividade ilegal, que não condiga com as atividades a serem cumpridas ou que possa causar prejuízo ao bom funcionamento da infraestrutura de TIC deste Poder, a exemplo, mas não se limitando a: I - Arquivos de mídia, softwares e demais materiais protegidos por propriedade intelectual sem a devida licença ou autorização.
Proibição de conteúdos pessoais, pornográficos, ilícitos.	**Art. 27 da PSI -** É vetado aos agentes do judiciário acessar ou armazenar, a partir de dispositivos ou recursos de TIC do TJPE ou pessoais em seu proveito, conteúdo que caracterize atividade ilegal, que não condiga com as atividades a serem cumpridas ou que possa causar prejuízo ao bom funcionamento da infraestrutura de TIC deste Poder, a exemplo, mas não se limitando a: II - Material pornográfico ou que possua intenção de satisfazer a lascívia; IV - Conteúdos ou serviços de TIC de ordem pessoal dos agentes judiciários ou de terceiros, tais quais, repositórios de arquivos na internet, serviço de e-mail, mídias sociais não liberadas, rádios online e recursos de entretenimento em geral; V - Que constitua crime, ato ilícito ou contrarie a Ordem Pública, os bons costumes, as Normas em vigor do TJPE ou seus objetivos e função social.

Alteração dos Normativos

Indicador	Nova Cláusula
Proibição de coleta de fotos e imagens no perímetro físico da empresa bem como de sua publicação sem autorização prévia da empresa.	**Art. 26 da PSI -** Não é permitido aos agentes judiciários tirarem fotos, capturarem imagens, som ou vídeo do ambiente compreendido no perímetro físico sob gerenciamento deste Poder ou divulgar esses materiais sem uma autorização prévia da instituição.
Aviso claro e objetivo de Inspeção Física (alcançando também dispositivos particulares dentro do perímetro físico).	**5.7.2. da Norma de Recursos de TIC -** O TJPE se reserva o direito de forma irrestrita e sempre que considerar necessário auditar e realizar inspeções físicas nos dispositivos de mobilidade, equipamentos, sistemas ou recursos que interajam com seus ambientes lógicos e/ou físicos. Também, supervisiona seus dados e informações, sobretudo nos recursos de TIC de propriedade de terceiros quando autorizada a entrada em suas instalações, independentemente da interação com seus ambientes e informações, pelos princípios de prevenção e proteção ao negócio.

Alteração dos Normativos

Indicador	Nova Cláusula
Aviso claro e objetivo de Monitoramento irrestrito (alcançando também dispositivos particulares dentro do perímetro físico e lógico).	**Art. 25 da PSI -** Este Poder monitora todos os recursos, ambientes, dispositivos e ativos ligados à Tecnologia de Informação e Comunicação, tais como, mas não se restringindo ao e-mail institucional, acesso à internet, estrutura de comunicação telefônica, espaços físicos e utilização dos dispositivos de TIC institucionais, com a finalidade de proteger seus ativos, sua reputação e conhecimento. **Parágrafo Primeiro –** Este Poder também registra todos os dados obtidos pelo monitoramento realizado para eventual análise forense, apuração a violações à Estrutura Normativa de Segurança de Informação ou investigar fatos que comprometam seus ativos.

Alteração dos Normativos

Indicador	Nova Cláusula
Dever de mobilidade segura independente de quem fornece o dispositivo (conforme nova regra do art. 6º. da CLT), bastando que seja informação da empresa (inclui uso de bloqueio de acesso (seja celular, pendrive, notebook ou tablet), dever de criptografia, dever de backup, vedação para envio de conteúdo corporativo para caixa postal de e-mail particular, vedação de uso de pastas de compartilhamento gratuito de arquivos de forma pública como Dropbox e Slideshare), vedação para uso de 3G e navegação em paralelo (fora do firewall) se não tiver sido autorizado, orientação sobre uso de rede wi-fi.	**Para atender este indicador elaboramos a Norma para Uso dos Dispositivo de Mobilidade, que contempla todas as recomendações a exemplo de:** **5.3.1. da Norma de Disp. Mobilidade -** Quando o dispositivo de mobilidade for fornecido pelo TJPE, os agentes judiciários e demais colaboradores devem realizar cuidados básicos de segurança, a exemplo, mas não se limitando ao backup (cópias de segurança) das informações da instituições, varredura de vírus e conectá-lo periodicamente à rede corporativa para atender procedimentos rotineiros de checagem de conformidade.

Alteração dos Normativos

Indicador	Nova Cláusula
Orientação sobre o acesso seguro ao invés de portar dados (deve portar sempre menor quantidade possível pelo menor tempo, apenas o estritamente necessário e sempre em dispositivo com bloqueio de acesso).	**5.11.1 da Norma de Disp. Mobilidade -** Os agentes judiciários e demais colaboradores devem armazenar as informações geradas a partir do dispositivo de mobilidade ou acesso remoto na rede corporativa.
Aviso que o mero acesso ao recurso pode ocorrer de forma remota e a qualquer horário e, por si só, não configura sobrejornada nem hora extra.	**5.1.7. da Norma de Disp. Mobilidade -** Não implicará em sobrejornada, sobreaviso ou plantão do agente judiciário ou colaboradores a mera possibilidade de acesso remoto, porte ou uso dos dispositivos de mobilidade fornecidos pelo TJPE ou particular quando utilizados para finalidades profissionais, pois estes permanecem ativos e disponíveis independentemente da vontade do agente judiciário ou comando da instituição. Assim, as atividades desempenhadas fora do expediente normal dependerão de comprovação em registros adequados para serem remuneradas.

Alteração dos Normativos

Indicador	Nova Cláusula
Orientação sobre postura em Redes Sociais (independente do tipo de conexão e do tipo de perfil, se corporativo ou pessoal), tratando sobre uso de marca, informações de rotina de trabalho, tratamento respeitoso e ético com os colegas.	**Art. 28 da PSI -** Este Poder aconselha aos agentes judiciários que utilizarem as Mídias Sociais a evitar expor rotinas de trabalho e de demais detalhes privados e íntimos sobre si, família, amigos próximos. Também, se sugere que utilizem somente conteúdos autorizados com a citação da fonte, para evitar punições por crimes contra direitos autorais ou que firam direitos de marca e não faltem com educação, polidez e urbanidade quando forem interagir com os demais usuários.
Dever de denúncia imediata de incidente.	**Art. 50 da PSI -** Todos os agentes judiciários devem noticiar à Ouvidoria os incidentes de Segurança da Informação que presenciarem ou tomarem conhecimento, ainda que por mera suspeita, para que a providência adequada seja adotada no menor tempo possível e minimizando os danos sofridos por este Poder, sem prejuízo de comunicação administrativa conforme o caso e urgência, formalmente.

Alteração dos Normativos

Indicador	Nova Cláusula
Responsabilidade do gestor sobre os recursos e postura de sua equipe.	**Art. 28 da PSI -** Este Poder aconselha aos agentes judiciários que utilizarem as Mídias Sociais a evitar expor rotinas de trabalho e de demais detalhes privados e íntimos sobre si, família, amigos próximos. Também, se sugere que utilizem somente conteúdos autorizados com a citação da fonte, para evitar punições por crimes contra direitos autorais ou que firam direitos de marca e não faltem com educação, polidez e urbanidade quando forem interagir com os demais usuários.
Aviso de que a tentativa de burlar será considerada também infração.	**Processo Disciplinar (Esta cláusula contém em todas as Normas) -** O agente judiciário ou colaborador que tomar atitudes ou ações contrárias ao estabelecido por esta Norma, ainda que por mera tentativa de burla, estará sujeito às possíveis penalidades administrativas, sem prejuízo de ações legais cabíveis. Estas violações serão avaliadas tanto quanto a responsabilidade pessoal como quanto a institucional.

Alteração dos Normativos

Indicador	Nova Cláusula
Responsabilidade do gestor sobre os recursos e postura de sua equipe.	**Art. 8°, IV -** Cabe às chefias a responsabilidade por gerir os recursos de TIC e postura dos agentes judiciários que compõem sua Área ou equipe em relação a Segurança da Informação. **OBS: Esta Cláusula contém em todas as Normas.**
Aviso de que a tentativa de burlar será considerada também infração.	**Processo Disciplinar -** O agente judiciário ou colaborador que tomar atitudes ou ações contrárias ao estabelecido por esta Norma, ainda que por mera tentativa de burla, estará sujeito às possíveis penalidades administrativas, sem prejuízo de ações legais cabíveis. Estas violações serão avaliadas tanto quanto a responsabilidade pessoal como quanto a institucional. **OBS: Esta Cláusula contém em todas as Normas.**

Alteração dos Normativos

Indicador	Nova Cláusula
Informação de que a empresa irá colaborar com as autoridades.	**Art. 42 da PSI -** Ao TJPE é facultada a realização de análises de conformidade ou auditorias periódicas na segurança da infraestrutura de TIC, seus ativos, processos e pessoas com o objetivo de detectar vulnerabilidades e demonstrar evidências do cumprimento da política e boas práticas de segurança da informação.
Dever de Educação e Conscientização.	**Art. 14, I da PSI -** Cabe ao Núcleo de Segurança da Informação da SETIC promover Campanhas com o objetivo de conscientizar os agentes judiciários sobre a Estrutura Normativa de Segurança da Informação.
Dever de guarda das provas.	**Art. 44 da PSI -** A SETIC tem o dever de guardar as provas produzidas pelos recursos e dispositivos de TIC pelo tempo previsto na tabela de temporalidade deste Poder, sobretudo em casos de incidente de Segurança de Informação.

Alteração dos Normativos

Indicador	Nova Cláusula
Dever de observar questões de segurança da informação no processo de seleção de pessoas.	**Art. 36, Parágrafo Primeiro da PSI -** Os responsáveis pela contratação ou seleção de colaboradores e agentes judiciários deverão utilizar de todos os meios legais para análise e observação de reputação dos mesmos, podendo realizar levantamento completo de informações e referências através de pesquisas na internet e Mídias Sociais, inclusive, mas sempre pautando-se pela ética e proporcionalidade.
Aviso de penalidades.	**Art. 51 da PSI -** Violações desta Política de Segurança de Informação, Normas e Procedimentos correlatos são passíveis de penalidades administrativas, sem prejuízo de ações legais cabíveis. Estas violações serão avaliadas tanto quanto a responsabilidade pessoal como quanto a institucional.
Obrigação de formação e atuação do Comitê de Segurança da Informação.	**Art. 10° da PSI consta as responsabilidades do Comitê Gestor de TIC. A Exemplo de:** Propor alterações nesta Política e as comunicar ao Tribunal Pleno e analisar os casos de violação e incidentes.

Alteração dos Normativos

Indicador	Nova Cláusula
Informação onde encontrar os documentos de Segurança da Informação.	**Art. 52 da PSI -** Todos os documentos da Estrutura Normativa de Segurança da Informação do TJPE estão disponibilizados em [indicar caminho da intranet ou internet]. **OBS: Esta Cláusula contém em todas as Normas.**
Dever do colaborador se manter sempre atualizado e ciente das normas da empresa.	**Art. 7°, III da PSI -** Cabe aos agentes do judiciário estar sempre atualizado e ciente das Políticas, Normas e Procedimentos vigentes do TJPE ou do órgão subordinado que executar suas tarefas. **OBS: Esta Cláusula contém em todas as Normas.**
Obrigatoriedade de uso de recursos de segurança (antivírus, firewall).	**5.2.4. da Norma para Recursos de TIC -** Os recursos de TIC, inclusive os móveis ou portáteis, deverão dispor de softwares de proteção devendo permanecer sempre instalados, ativos e atualizados, a exemplo, mas não se limitando a antivírus, antispyware e firewall.

Alteração dos Normativos

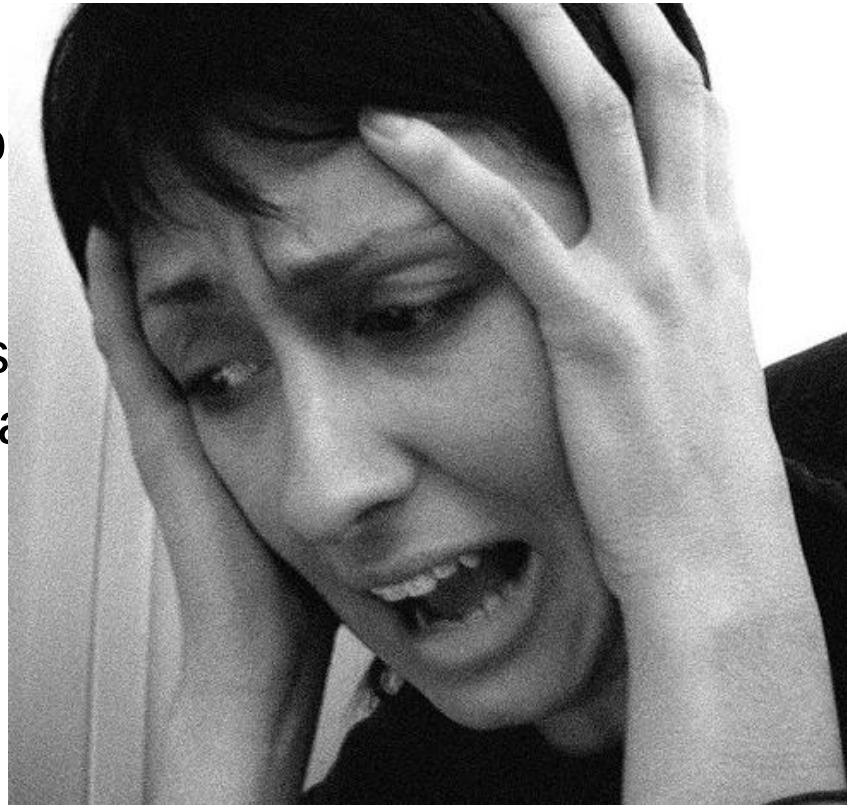
Indicador	Nova Cláusula
Glossário de Termos técnicos.	**Atualizamos o Glossário Geral de Termos.**
Dever de atualização periódica do documento (em intervalo não superior a 2 anos).	Esta Norma deve ser revista e atualizada anualmente, visando à garantia que todos os requisitos de segurança técnicos e legais implementados estejam sendo cumpridos, atualizados e em conformidade com a legislação vigente. **OBS: Esta Cláusula contém em todas as Normas.**
Recomendações para proteção contra Engenharia Social.	**Art. 7º, X da PSI –** Cabe aos agentes judiciários estar atento ao repassar ou transmitir informações para outras pessoas, seja de forma presencial, via telefone, comunicadores instantâneos, mensagens eletrônicas ou mídias sociais. Confirme sempre a identidade e idoneidade do solicitante ou destinatário antes do envio de informações e, sempre que possível, a real necessidade do compartilhamento de alguma informação solicitada por outra pessoa, mesmo que de sua confiança.

CUIDADO COM O TECNOESTRESSE

faça uso saudável da tecnologia

- ✓ Na maioria dos casos estudados, o problema surge quando a pessoa não consegue usar os equipamentos de maneira equilibrada, não sabe lidar com eles, não compreende como eles funcionam e, principalmente, quando a tecnologia falha.

- ✓ **Sintomas: ansiedade, irritação, agressividade, insônia, depressão, distúrbios alimentares.**



Fonte: Revista Vida e Saúde (http://revistavivasaude.uol.com.br/edicoes/38/artigo40186-1.asp). Imagem: Nate Steiner (http://www.flickr.com/photos/nate/321938695/. Acesso em 16/10/2012

O Hospital das Clínicas de SP criou, em 2006, um programa para tratamento dos viciados em internet

Dúvidas?

Muito obrigado!

http://www.leitecommangafazmal.com.br/site/wp-content/uploads/2011/06/tira-duvidas1.jpg

Dra. Patricia Peck Pinheiro sócia fundadora

- Advogada formada pela Universidade de São Paulo
- Especialização Negócios Harvard Business School
- Gestão de Riscos pela Fundação Dom Cabral
- MBA Marketing Madia Marketing School
- Formada pela Escola de Inteligência do Exército Brasileiro
- Sócia Fundadora do escritório Patricia Peck Pinheiro Adv
- Árbitra do Conselho Arbitral do Estado de São Paulo – CAESP
- Idealizadora do Movimento Família Mais Segura na Internet
- Condecorada com Medalha do Pacificador pelo Exército em 2009
- Condecorada com Medalha Tamandaré pela Marinha em 2011
- Condecorada com Medalha Ordem do Mérito Militar pelo Exército em 2012
- Recebeu o Prêmio "Security Leaders" por seus trabalhos de Educação e Conscientização em Segurança Digital em 2012
- Recebeu o Prêmio "Advogada Mais Admirada em Propriedade Intelectual" em 2010 , 2011 e 2012
- Recebeu o Prêmio "A Nata dos Profissionais Segurança Informação" em 2006 e 2008
- Recebeu o Prêmio "Excelência Acadêmica – Melhor Docente da faculdade FIT Impacta" em 2009 e 2010
- Programadora desde os 13 anos, com experiência EUA, Portugal e Coréia
- Autora do livro Direito Digital, já na 5ª. edição (www.saraiva.com.br)
- Organizadora do Livro Direito Digital Aplicado
- Coautora dos audiolivros Direito Digital no Dia-a-Dia, Direito Digital Corporativo e Eleições Digitais
- Coautora do ebook iMarketing Direito Digital na Publicidade (http://itunes.apple.com/br/)
- Coautora dos livros "e-Dicas", "Internet Legal" e "Direito e Internet II";
- Coautora dos livros "Novas Competências na Sociedade do Conhecimento" e "Os ´Novos´ Direitos no Brasil"
- Colunista do IDG Now, Revista Visão Jurídica, Revista PartnerSales, Programa Conta Corrente da Globonews.

Principais Prêmios

2011

2012

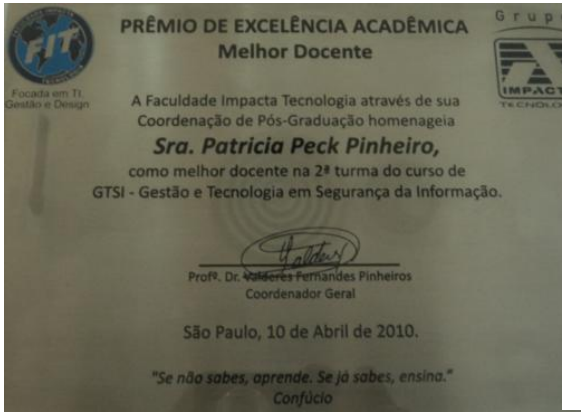
2012

2006

2009

2010

2010



Principais Medalhas

Formadores de Opinião

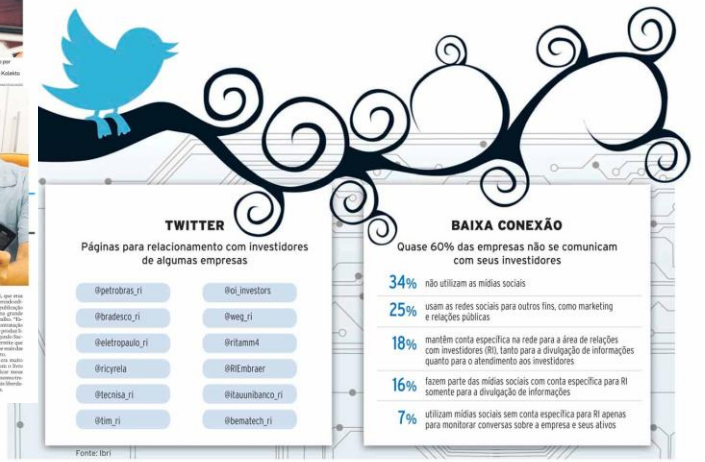
INFORMÁTICA

Utilização de software pirata recuou 11 pontos percentuais nos últimos sete anos

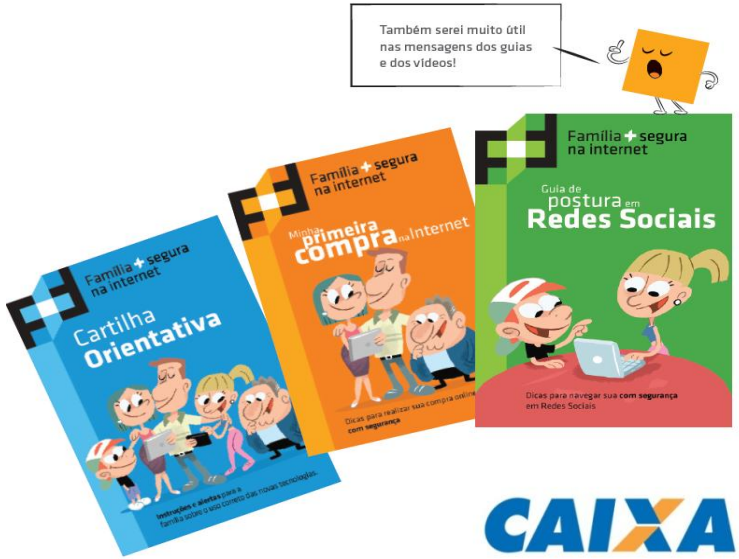
Redes sociais: o centro das atenções

Sandra Paula Tomazi Weber*

Direito digital Empregados si
Mau uso da



Acesse: www.familiamaissegura.com.br



http://www.facebook.com/FamiliaMaisSeguraNaInternet

:.com/FamiliaMaisSegu

Contato: Cida
(55 11) 3068-0777
(55 11) 99789-8222
presidencia@istart.org.br

AGENDA DE TREINAMENTOS

Março/2013

Consumidor Online e Comércio Eletrônico

20/03– 10h às 17h

Abril /2013

Redes Sociais Aspectos Legais

24/04– 10h às 17h

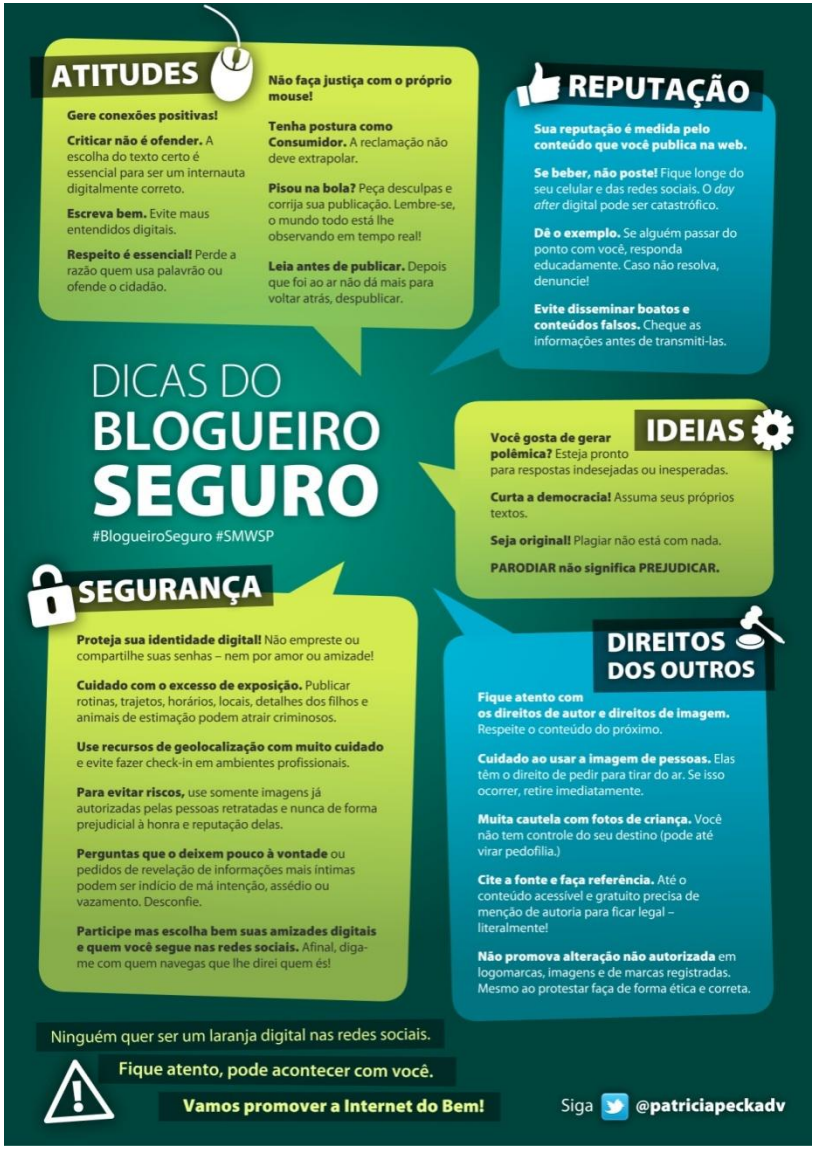
Maio /2013

Direito Digital Aplicado

22/05– 10h às 17h

WWW.PPPADVOGADOS.COM.BR

Assine a nossa newsletter mensal!



Vamos promover a Internet do Bem!

http://twitpic.com/8h84ht

Facebook: http://ow.ly/95QAU