RISCOS CONTRA A INTEGRIDADE, AUTENTICIDADE E CONFIDENCIALIDADE DE DOCUMENTOS DIGITAIS

João Batista Ribas de Moura*

Resumo

Ambientes inseguros podem levar a incidentes que demonstram as limitações da tecnologia de assinatura digital quando não acompanhadas de outras medidas de segurança. Conhecer cenários onde uma assinatura é produzida sem o consentimento de seu proprietário é fundamental para uma melhor compreensão do significado de "não-repúdio" e de como a integridade, autenticidade ou confidencialidade poderiam ser comprometidas. Este estudo corrobora o veto ao artigo do projeto de lei que permitiria a destruição do documento original em papel após sua digitalização.

A conversão da fiel imagem de um documento em papel para seu equivalente digital, também chamada de digitalização, transformando-o em documento digital[1] para posterior acesso e armazenamento em sistema computacional já é realidade em organizações públicas e privadas de todo o mundo.

A pressão por redução de custos e por aumento da velocidade na tramitação de processos faz surgir um mundo virtualizado com seus documentos, identidades e assinaturas digitais, que impõem um novo olhar crítico para que se mantenha a segurança das informações também nesse novo paradigma. O objetivo deste artigo é demonstrar situações que levam à violação da confidencialidade ou à quebra da integridade e autenticidade de documentos digitais, alertando, inclusive, para os riscos envolvidos na tecnologia de assinatura digital em ambientes inseguros.

O documento digital tornou-se forte aliado da Lei de Acesso à Informação[2] porque essa nova legislação norteia-se pelo uso de tecnologias da informação

* Analista Tributário da Receita Federal do Brasil. Bacharel em Administração de Empresas; MBA em Administração Estratégica de Sistemas de Informação (FGV); Mestrando em Computação Aplicada: gestão de riscos (UnB); Membro do Comitê Gestor de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República (GSI/PR).

1 O Documento digital pode nascer de duas formas: a partir da imagem obtida de um original em papel (digitalização) ou já nascer digital quando gerado dentro de sistema computacional como ocorre, por exemplo, na criação de documento com editor de textos. Neste último caso, o texto nasce e se mantém em ambiente sem a necessidade de ser materializado em papel (impresso).

2 Lei n° 12.527/2011, de 18 de novembro de 2011 e vigência desde 16 de maio de 2012 (BRASIL, 2011).

A pressão por redução de custos e por aumento da velocidade na tramitação de processos faz surgir um mundo virtualizado com seus documentos, identidades e assinaturas digitais, que impõem um novo olhar crítico para que se mantenha a segurança das informações também nesse novo paradigma.

como facilitadora do acesso à informação. O necessário fortalecimento da cultura de informação digital ocorre a partir de ações do governo federal como, por exemplo, a Resolução nº 20, de 16 de julho de 2004, do Conselho Nacional de Arquivos (Conarq), que dispõe sobre a inserção dos documentos digitais em programas de gestão arquivística de documentos dos órgãos e entidades integrantes do Sistema Nacional de Arquivos (BRASIL, 2004); o Plano Nacional de Desmaterialização de Processos (PND-Proc) (BRASIL, 2011) e a Lei nº 12.682, de 9 de julho de 2012, que regulamentou a elaboração e o arquivamento de documentos em meios eletromagnéticos (ênfase adicionada):

> O processo de digitalização deverá ser realizado de forma a manter a **integridade, a autenticidade** e, se necessário, **a confidencialidade** do documento digital, **com o emprego de certificado** digital emitido no âmbito da **Infraestrutura de Chaves Públicas Brasileira** - ICP - Brasil. (BRASIL, 2012a, art. 3º, grifo nosso).

A reconhecida natureza volátil e a facilidade de manipulação inerente ao meio digital remetem ao uso da tecnologia de assinatura digital para garantir a autenticidade e a integridade dos documentos em meio eletromagnético. Da mesma forma que uma assinatura manuscrita em papel possui traços únicos associados ao seu autor (signatário), a assinatura digital é criada a partir de um "Certificado Digital[3]" que nada mais é do que outro documento digital contendo características únicas associadas ao seu proprietário (pessoa física ou jurídica). É uma espécie de "carteira de identidade digital" concedida por Autoridade Certificadora que cria e grava o certificado digital preferencialmente em dispositivo portátil de armazenamento, conhecido como *token* ou *smartcard*. O acesso a esse dispositivo para executar o procedimento de assinatura digital é feito mediante uso de senha secreta de conhecimento exclusivo de seu proprietário.

Cabe ao ICP-Brasil[4] fiscalizar e auditar os processos de emissão de certificados digitais executados pelas autoridades certificadoras garantindo confiabilidade

[3] Mais precisamente, um certificado digital contém em seu interior dois grupos de informações: a chave privada e a chave pública. A chave privada deve ser utilizada por seu proprietário nos procedimentos matemáticos aplicados sobre o documento (que está) sendo assinado digitalmente. A veracidade da assinatura pode ser confirmada por qualquer pessoa utilizando-se a respectiva chave pública.

[4] A Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) mantém a Infraestrutura de Chaves Públicas Brasileira, que é auditada e mantida pelo Instituto Nacional de Tecnologia da Informação (ITI).

e presunção legal de todos os procedimentos envolvidos.

A robustez das operações matemáticas envolvidas na assinatura digital dá ao documento digital a característica de íntegro e autêntico, daí se apresentando o conceito de "**não-repúdio**". Isto é, ninguém pode repudiar o resultado matemático gerado ou negar que tenha sido calculado a partir de dados contidos em determinado certificado digital. Essa expressão é **erroneamente levada ao "mundo jurídico**" como se fosse impossível que uma assinatura digital pudesse ter sido empregada sem o consentimento de seu real proprietário.

> 19) Não-repúdio, porém, é uma expressão técnica, que diz respeito à vinculação do par de chaves criptográficas. Bruce Schneier já alertava para a apropriação indevida que a indústria PKI[5] fez da expressão, para dar a seus produtos algum significado jurídico, por mais absurdo que fosse.
>
> Impedir alguém de negar uma assinatura, digital ou não, é a negação do Estado de Direito. Pode-se regular ônus de prova de quem negar uma assinatura, mas jamais retirar de alguém o direito de impugná-la.
>
> 20) De outra parte, não-repúdio nada tem a ver com emissão de certificados, estando restrito à relação existente entre o par de chaves criptográficas. O fato de existir certificado, ou desse certificado ser emitido no âmbito da ICP-Brasil, nenhuma relação ter a ver com o não-repúdio. (COSTA, 2003, p.7).

Comparando-se a assinatura digital com a assinatura manuscrita aplicada, por exemplo, em escritura pública na presença de tabelião, percebe-se que nesta há verificação precisa da identidade e da vontade de quem assina, enquanto naquela tais aspectos são confiados a um ambiente computacional cuja integridade e segurança podem não estar presentes.

> [...] § 1º Salvo quando exigidos por lei outros requisitos, a escritura pública deve conter:
>
> I - data e local de sua realização;
>
> II - reconhecimento da identidade e capacidade das partes e de quantos hajam comparecido ao ato, por si, como representantes, intervenientes ou testemunhas; [...]
>
> IV - **manifestação clara da vontade** das partes e dos intervenientes; [...]
>
> (BRASIL, 2002, art. 215º, grifo nosso)

Durante a execução da assinatura digital, o procedimento computacional aplicado não é ratificado por uma terceira pessoa e, obviamente, não há confirmação quanto à vontade de assinar. Existe apenas a garantia de que, em algum momento no passado, um determinado certificado digital foi entregue à pessoa corretamente identificada perante a Autoridade Certificadora. O ato de assinar digitalmente é "garantido" por uma máquina (computador), ou melhor, por um sistema constituído de *hardware* (partes sólidas/visíveis/mecânicas) e *software* (partes voláteis/invisíveis/elétricas ou programas/sistemas). Máquinas não "desconfiam de nada" porque ainda não pensam. Apenas obedecem cegamente a programação

[5] PKI significa Public-Key Infraestructure ou Infraestrutura de Chaves Públicas, que no Brasil chama-se ICP-Brasil e foi definida pela Medida Provisória 2.200-2, de 24 de agosto de 2001 (BRASIL, 2001).

que lhes foi dada. Por esta razão, *a priori*, a assinatura digital é realizada:

- Sem que o sistema computacional tenha certeza de que a pessoa que está a frente do equipamento fornecendo a senha correta é a mesma pessoa detentora do certificado digital sendo utilizado.
- Sem a compreensão da "manifestação clara da vontade" de quem está à frente do teclado porque um invasor poderia ter acesso físico aos equipamentos e também à senha secreta previamente capturada, conforme cenário de incidente adiante descrito.

Se o ambiente, residencial ou laboral, não for seguro, haveria **risco de um invasor capturar a senha que dá acesso ao smart card/token para posterior utilização ilegal?** Se o sistema computacional utilizado não for seguro, haveria **risco de um documento ser assinado sem o consentimento do legítimo proprietário do certificado digital utilizado?**

> Um dos maiores riscos de qualquer sistema baseado em Autoridade Certificadora está relacionado a sua própria chave privada de assinatura. Como você a protege? Você provavelmente não possui um sistema de computação seguro com controles de acesso físico, (...) e outras proteções. Você armazena sua chave privada em um computador convencional. Lá, ele está sujeito ao ataque de vírus e outros programas maliciosos. Mesmo que sua chave privada esteja a salvo em seu computador, ele está em uma sala fechada monitorada por circuito fechado de TV para ter a certeza de que ninguém mais tem acesso a ela? Se é protegido por senha, quão difícil é obtê-la? Se sua chave é armazenada em um *smart card*, quão resistente a ataques ele é (muitos são bastante fracos)? Se é armazenada em um dispositivo realmente resistente a ataques, poderia um computador infectado conduzir o dispositivo de armazenamento da chave privada para assinar um documento que você não tinha intenção de assinar? [...] (ELLISON, 2000, p.2)

O cenário de incidente onde um invasor obtém acesso ao ambiente de trabalho e **adultera um documento digital** e, com uso de *smart card/token* deixado na gaveta durante o horário de almoço, **utiliza-se da senha de acesso previamente capturada,** executando o procedimento de assinatura digital em nome de outrem, **é possível em organizações com pouca ou nenhuma cultura de segurança** institucional e despreparo contra técnicas de Engenharia Social.

A informação tornou-se um ativo como qualquer outro e o avanço das tecnologias computacionais tornaram o universo das invasões eletrônicas cada vez mais sofisticado.

Esse tipo de cenário é factível porque o ser humano é o elo mais frágil a ser trabalhado na segurança da informação. Kevin Mitnick – um dos mais conhecidos cibercriminosos da história dos EUA – invadia sistemas computacionais com uso da 'Engenharia Social', jargão do mundo tecnológico usado para descrever a arte de explorar o desconhecimento e a ingenuidade humana para a obtenção de informações e acessos restritos. (MOURA, 2010, p.21).

Mogull (2002), analista do Gartner, alerta que a "**Engenharia Social é a maior ameaça à segurança corporativa**", além de que "as falhas de segurança mais prejudicais são devidas à Engenharia social e não à invasões eletrônicas".

Mitknick e Simon (2003, p. 7) citam, ainda, que "não somos treinados para suspeitarmos uns dos outros. Somos ensinados a "amar o próximo" e a ter confiança e fé uns nos outros. Como uma nação, incorporamos ao nosso conceito de liberdade a ideia de que o melhor lugar para viver é aquele sem cadeados e chaves".

A informação tornou-se um ativo como qualquer outro e o avanço das tecnologias computacionais tornaram o universo das invasões eletrônicas cada vez mais sofisticado. A *European Network and Information Security Agency* (ENISA) e a *Organisation for Economic Co-Operation and Development* (OECD) afirmam que "**a conscientização dos riscos e das medidas de segurança disponíveis são a primeira linha de defesa para a segurança dos sistemas de informação** e redes". (ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, 2002, p.10, grifo nosso).

Em ambiente onde há vulnerabilidade pela falta de cultura e despreparo com as questões relativas à segurança institucional, a ameaça constante de ataques com uso de Engenharia Social aumenta o risco de uma invasão bem-sucedida que vise, por exemplo, o acesso físico ao ambiente laboral para instalação de dispositivo de captura de senhas.

Outro cenário de incidente possível ocorre quando controles de acesso físico são inexistentes ou ineficientes. Neste caso, um invasor acessaria o ambiente laboral para executar diversas atividades ilegais como, por exemplo: furto de mídias; ataques contra equipamentos servidores; escuta da comunicação trafegando em rede; adulteração de documentos digitais no ato da assinatura pelo comprometimento do sistema computacional e manipulação da imagem apresentada na tela (monitor de vídeo).

> O rápido avanço das tecnologias de segurança computacionais tem feito com que as invasões eletrônicas tornem-se incrivelmente mais difíceis aos *hackers*, portanto, **nós veremos crescer a implementação de métodos de ataque à segurança física**. (ALLSOPP, 2009, p. XVIII, grifo nosso).

A Segurança Física é frequentemente negligenciada em favor de aspectos mais técnicos como vírus, *trojans*, *spywares*, *hacking*, etc. Sem ela, há risco de furto, dano ou modificações não autorizadas aos sistemas em equipamentos servidores.

> Pessoas de dentro da organização podem explorar a maioria das brechas de segurança. **É muito mais fácil invadir um sistema de dentro da organização do que de fora porque você não terá que passar pelos perímetros de defesa (usualmente *firewalls*)**. Hackear um sistema é muito mais fácil se você tiver acesso físico a ele. Há muitas ferramentas *hackers* que permitem inclusive a amadores, com um mínimo de experiência em redes computacionais, invadir um equipamento servidor em minutos se existir acesso físico a rede interna. (POSEY, 2003, grifo nosso).

Josang (2008), em seu artigo *'What You See Is Not Always What You Sign'* (o que você vê nem sempre é o que você assina), demonstra cenários onde um sistema computacional é comprometido (invadido e alterado) fazendo com que o usuário assine um documento digital mostrado em tela, enquanto, na verdade, está assinando outro documento:

> O termo "assinatura digital" é uma metáfora que pode levar as pessoas a acreditarem que existe equivalência com a assinatura à mão. No entanto, deve ser visto como um novo paradigma adequado aos sistemas computacionais em vez de tratá-lo como equivalente à assinatura manuscrita. [...]

A Norma ABNT NBR ISO/IEC 27001:2005 define os controles de segurança adequados e proporcionais objetivando a proteção dos ativos da informação. O controle "A.9.1" objetiva "**prevenir o acesso físico não autorizado**, danos e interferências contra as instalações e informações da organização". No controle "A.9.1.2 – Controles de entrada física" tem-se: "**As áreas seguras devem ser protegidas por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso**." (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2005, grifo nosso)

> **Um dos princípios da segurança física mais desafiador é: "você deve interpelar qualquer um que não esteja usando um crachá válido**". Pessoalmente eu acho isso extremamente difícil – provavelmente porque eu gosto de ser gentil com os outros. O resultado é um confronto de decisão entre as regras e o modelo mental normal. (MCILWRAITH, 2006, grifo nosso)

A Norma Complementar nº 07/IN01/DSIC/GSIPR, de 06 de maio de 2010, do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República, objetiva "estabelecer diretrizes para implementação de **controles de acesso relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF**" (BRASIL, 2010, grifo nosso), e deveria ser seguida para diminuir a probabilidade de ocorrência de incidente de segurança de acesso físico não autorizado com possibilidade de comprometimento dos sistemas relacionados ao Gerenciamento Eletrônico de Documentos[6] (GED).

A Norma Complementar nº 04/IN01/DSIC/GSIPR (BRASIL, 2009) estabelece diretrizes para o processo de **Gestão de Riscos de Segurança da Informação e Comunicações** (GRSIC) nos órgãos ou entidades da Administração Pública Federal, sendo importante para ajudar na detecção de ameaças e vulnerabilidades remanescentes após a implementação de controles de segurança corretivos.

É oportuno observar que se há risco de incidente que possa comprometer a autenticidade e a integridade de documentos digitais então a manifestação do Ministério da Justiça que embasou **os vetos**

[6] Conjunto de tecnologias responsáveis por gerar, manter e disponibilizar documentos digitais.

aos artigos 2º, 5º e 7º do Projeto de Lei nº 11, de 2007 [7], é bastante pertinente quando analisada sob a ótica dos riscos de segurança já exemplificados e cuidadosamente embasados neste artigo.

> [...] Ouvido, o Ministério da Justiça manifestou-se pelo **veto aos seguintes dispositivos**:
>
> **Arts. 2º, 5º e 7º**
>
> "[...]
>
> § 1º Após a digitalização, constatada a integridade do documento digital, **o original poderá ser destruído**, ressalvados os documentos de valor histórico, cuja preservação deverá observar a legislação pertinente.
>
> § 2º O documento digital e a sua reprodução, em qualquer meio, procedida de acordo com o disposto nesta Lei **terão o mesmo valor probatório do documento original, para todos os fins de direito**.
>
> Art. 5º Decorridos os respectivos prazos de decadência ou prescrição, os documentos armazenados em meio eletrônico, óptico ou equivalente **poderão ser eliminados**.
>
> Art. 7º Os documentos digitalizados nos termos desta Lei terão o mesmo efeito jurídico conferido aos documentos microfilmados, consoante a Lei no 5.433, de 8 de maio de 1968, e regulamentação posterior."
>
> Razões dos vetos:
>
> "Ao regular a produção de efeitos jurídicos dos documentos resultantes do processo de digitalização de forma distinta, **os dispositivos ensejariam insegurança jurídica**. Ademais, as autorizações para destruição dos documentos originais logo após a digitalização e para eliminação dos documentos armazenados em meio eletrônico, óptico ou equivalente não observam o procedimento previsto na legislação arquivística [...]" (BRASIL, 2012b, grifo nosso).

Embora alguns fervorosos e apaixonados profissionais do Gerenciamento Eletrônico de Documentos critiquem os vetos supracitados porque inviabilizaram a destruição do documento original em papel, e também porque não conferiram ao documento digital o mesmo valor probatório do documento em papel, entende-se que tais vetos são medidas justificáveis sob a égide da segurança da informação.

Conclusão

Conclui-se que as inúmeras vantagens na utilização de documentos digitais podem ser obliteradas em ambientes onde os riscos de segurança possam materializar-se, a exemplo dos cenários de incidentes demonstrados neste artigo. Nesses casos, até mesmo a utilização de tecnologia de assinatura digital pode ser insuficiente para garantir a integridade e a autenticidade de documentos digitais. A confidencialidade também depende de ambientes com eficientes controles de acesso físico e pessoas sensibilizadas quanto às técnicas de engenharia social. Assim, espera-se que as organizações trabalhem na formação e na manutenção da cultura de segurança já recomendada em normas do governo federal que descrevem as melhores práticas de segurança da informação e comunicações.

[7] Deu origem à Lei n°12.682, de 9 de julho de 2012, que regulamenta a elaboração e o arquivamento de documentos em meios eletromagnéticos (BRASIL, 2012a).

Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *NBR ISO/IEC 27001*: *Tecnologia da informação: Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos.* Rio de Janeiro: ABNT, 2006.

ALLSOPP, WILL. *Unauthorised Access: Physical Penetration Testing for IT Security Teams.* West Sussex: John Wiley and Sons, 2009. 287 p.

BAARS, Hans et al. *The Basics of Information Security – A Practical Handbook.* [S.I.]: Exin, 2009. 29 p. Disponível em: <http://www.innovanube.com/docs/ISFS_book_English_Final_incl_index.pdf>.

BRASIL. Código civil (2002). Lei no 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm>.

BRASIL. Lei n. 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5o, no inciso II do § 3o do art. 37 e no § 2o do art. 216 da Constituição Federal; altera a Lei no 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei no 8.159, de 8 de janeiro de 1991; e dá outras providências. *Diário Oficial da República Federativa do Brasil,* Poder Executivo, Brasília, DF, 18 nov. 2011, n. 132, Edição Extra, Seção 1, p. 1.

BRASIL. Lei n. 12.682, de 9 de julho de 2012a. Dispõe sobre a elaboração e o arquivamento de documentos em meios eletromagnéticos. *Diário Oficial da República Federativa do Brasil*, Poder Executivo, Brasília, DF, 10 jul. 2012, n. 132, seção 1, p. 1.

BRASIL. Medida Provisória n° 2.200-2, de 24 de agosto de 2001. Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia e dá outras providências. *Diário Oficial da República Federativa do Brasil,* Poder Executivo, Brasília, DF, 27 ago 2001, n. 164-E, seção 1, p. 65.

BRASIL. Mensagem nº 313, de 9 de julho de 2012b. Mensagem de veto à Lei nº 12.682, de 9 de julho de 2012. Disponível em <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Msg/ VEP-313.htm>. Acesso em: 31 ago. 2012.

BRASIL. Arquivo Nacional. Conselho Nacional de Arquivos. Resolução nº 20, de 16 de julho de 2004. Dispõe sobre a inserção dos documentos digitais em programas de gestão arquivística de documentos dos órgãos e entidades integrantes do Sistema Nacional de Arquivos. Disponível em: <http://www.conarq.arquivonacional.gov.br/cgi/cgilua.exe/sys/start.htm?infoid=71&sid=46>.

BRASIL. Gabinete de Segurança Institucional. Departamento de Segurança da Informação. Norma Complementar n° 04, de 14 de agosto de 2009. Estabelecer diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC nos órgãos ou entidades da Administração Pública Federal – APF, direta e indireta. *Diário Oficial da República Federativa do Brasil*, Poder Executivo, Brasília, DF, n. 156, 17 ago. 2009. Seção 1, p. 6. Norma Complementar à IN Nº 01/GSI/PR/2008 - Segurança da Informação e Comunicações).

BRASIL. Gabinete de Segurança Institucional. Departamento de Segurança da Informação. Norma Complementar n° 07, de 06 de maio de 2010. Estabelecer diretrizes para implementação de controles de acesso relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF. *Diário Oficial da República Federativa do Brasil*, Poder Executivo, Brasília, DF, n. 134, 16 jul. 2014. Seção 1, p.2. Norma Complementar à IN Nº 01/GSI/PR/2008 - Segurança da Informação e Comunicações.

BRASIL. Ministério do Planejamento, Orçamento e Gestão. *Planejamento Assina Acordo para Desburocratizar Administração Pública*. Brasília, 2011. Disponível em: <http://www.planejamento. gov.br/noticia.asp?p=not&cod=7942&cat=94& sec=7>. Acesso em: jul. 2012.

COSTA, Marcos da. Validade jurídica e valor probante de documentos eletrônicos. In: FÓRUM SOBRE SEGURANÇA, PRIVACIDADE E CERTIFICAÇÃO DIGITAL, 1., outubro de 2003, Brasília. *Fórum...* Brasília: Instituto Nacional de Tecnologia da Informação/Casa Civil da Presidência da República. Brasília, 2003.

ELLISON Carl; SCHNEIER, Bruce. Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure. *Computer Security Journal*, v. 16, n. 1, p. 1-7, 2000. Disponível em <http://www. schneier. com/paper-pki.html>. Acesso em: 31 ago. 2012.

JOSANG, Audun; ALFAYYADH, Bander. Robust WYSIWYS: a method for ensuring that what you see is what you sign. In: AUSTRALASIAN INFORMATION SECURITY CONFERENCE (AISC'08), 6., 2008, Wollongong, Australia. *Proceedings...* Wollongong, 2008. Disponível em: < http://folk.uio.no/josang/papers/JA2008-AISC.pdf>. Acesso em: 30 jul. 2012.

MITNICK, Kevin D.; SIMON, William L. *A Arte de Enganar*. São Paulo: Pearson Mackron Books, 2003. 284 p.

MCILWRAITH, Angus. *Information Security and Employee Behaviour: How to Reduce Risk through Employee Education, Training and Awareness.* Hampshire: Gower Publishing, 2006. 169 p.

MOGULL, Rich. Human Security Issues: Managing People and Defending Against Social Engineering. In: GARTNER INFORMATION SECURITY (INFOSEC) CONFERENCE, Chicago, 2002. *[Proceedings…].* Chicago, 2002.

MOURA, João Batista Ribas de. Segurança da informação nas organizações. *Idéias em Gestão*, Brasília, n. 4, p. 20-23, nov. 2010.

ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security.* 2002. Disponível em: <http://www.oecd.org/ document/42/0,3343,en_2649_34255_15582250_ 1_1 _ 1_1,00. html> . Acesso em: jul. 2012.

POSEY, Brien M. *Don't overlook physical security on your network*. Abr. 2003. Disponível em: <http://www.techrepublic.com/article/dont-overlook-physical-security-on-your-network/5032930>. Acesso em: ago. 2011.