Ciência forense aplicada à tecnologia da informação: adoção de técnicas forenses pelos ciclos de vida de desenvolvimento de sistemas de informação

RAMSES HENRIQUE MARTINEZ
Faculdade de Tecnologia de São Paulo – FATEC – SP – Brasil
ramses@usp.br

Resumo – Este artigo analisa o processo de investigação de crimes cometidos no ambiente da Tecnologia da Informação e busca avaliar a adoção de técnicas forenses pelos ciclos de vida de desenvolvimento de sistemas de informação. A metodologia utilizada foi o estudo de casos múltiplos, o que permitiu ao pesquisador o aprofundamento em alguns aspectos do processo de investigação de crimes cibernéticos. Das técnicas forenses apontadas pela literatura específica, poucas são adotadas, o que pode dificultar o processo de investigação quando da ocorrência de eventual fraude. Não obstante, também não foram identificadas políticas e recomendações específicas para o processo de investigação de crimes cibernéticos.

Abstract – This article examines the process of investigating crimes committed in the environment of information technology and seeks to assess the adoption of forensic techniques for life cycle development of information systems. The methodology used was the multiple case study, which allowed for a deepening in some aspects of the investigation of cyber crimes. Of forensic techniques identified by the specific literature, few are adopted, which may hinder the investigation process upon the occurrence of fraud. However, neither policies were identified and specific recommendations for the process of investigation of cyber crimes.

Palavras-chave: Tecnologia de Informação, Ciência Forense, Ciclo de Vida de Desenvolvimento de Sistemas.

1. Introdução

Este artigo analisa a aplicação da ciência forense à Tecnologia da Informação e propõe a adoção de técnicas forenses pelos ciclos de vida de desenvolvimento de sistemas de informação. Para isso, este artigo parte da revisão da bibliografia existente sobre o tema e das questões a ele associadas e pretende analisar as técnicas forenses que permitem aumentar a eficácia e eficiência do processo de investigação de crimes cometidos no âmbito do ciclo de vida de desenvolvimento de sistemas de informação. A metodologia de pesquisa utilizada foi o estudo de casos múltiplos, o que permitiu ao pesquisador o aprofundamento em alguns aspectos do processo de investigação de crimes cometidos no âmbito da Tecnologia da Informação. A pesquisa empírica contemplou seis instituições financeiras e foi realizada com base em entrevistas realizadas com gestores de centro de desenvolvimento de sistemas de informação. Pela avaliação das técnicas forenses, este artigo não apenas poderá

auxiliar em sua implementação pelos ciclos de vida de desenvolvimento de sistemas de informação, como também poderá contribuir para aumentar a eficácia e eficiência do processo de investigação de crimes cibernéticos.

2. Problema de Pesquisa e Objetivo

A vida em sociedade está cada vez mais arraigada nas relações, comerciais ou não, que são estabelecidas entre as pessoas e os Estados. Isso ocorre não apenas dentro dos limites geográficos de cada país, como também globalmente. Nesse contexto, o advento da Internet potencializou o estabelecimento dessas relações em patamares até então inimagináveis, com o uso intensivo de sistemas de informação [1,2]. Todavia, se de um lado a Internet teve um efeito bastante positivo no fomento das relações empresariais e interpessoais, de outro maximizou as indesejáveis mazelas que, infelizmente, sempre acompanharam tais relações. Como se vê, a dupla potencialidade da Internet, ao mesmo tempo em que ampliou o desenvolvimento e uso de sistemas de informação que sustentam tais relações, criou um ambiente propício para a consecução de atos ilícitos, pela facilidade em praticá-los e pela "sensação de impunidade", atribuída a um aparente anonimato. Esse outro lado da dupla potencialidade da Internet poderia afetar negativamente os inúmeros benefícios trazidos por essa nova forma de estabelecer relações. Para minimizar esses efeitos negativos, a aplicação da ciência forense em sistemas de informação revela que o apontado "anonimato" é de fato apenas aparente. Corrêa [3] (p. 74) lembra que "*(...) um computador acessado sem permissão, ou que possua material ilícito armazenado, contém evidências que podem ser utilizadas contra criminosos*". A importância do estudo reside no fato de que muitos crimes relacionados a sistemas de informação poderiam ser solucionados com maior eficácia e eficiência se técnicas forenses tivessem sido incorporadas aos ciclos de vida de desenvolvimento de sistemas. Desse modo, o processo de investigação, planejado e realizado de acordo com as melhores práticas, contribui para a identificação da autoria e aplicação das sanções cabíveis, o que assegura e aumenta a confiança nas transações empresariais e interpessoais. Assim, o objetivo do presente trabalho é, a partir da revisão bibliográfica, analisar o processo de investigação de crimes cometidos no âmbito da Tecnologia da Informação e buscar avaliar a adoção de técnicas forenses pelos ciclos de vida de desenvolvimento de sistemas de informação.

3. Revisão bibliográfica

Essa revisão visa auxiliar na avaliação da adoção de técnicas forenses pelos ciclos de vida de desenvolvimento de sistemas de informação. Inicialmente, serão revistos os trabalhos pertinentes ao processo de investigação e perícia e, em seguida, será tratado, especificamente, o processo de investigação de crimes cibernéticos.

Posteriormente, serão estudados os ciclos de vida de desenvolvimento de sistemas de informação e, finalmente, será analisada a adoção de técnicas forenses em tais ciclos de vida.

3.1. Investigação e Perícia

De acordo com Houaiss e Villar [4] (p.1644), investigação é o "*ato ou efeito de investigar*". Na esfera policial, a investigação consiste na "*averiguação sistemática de algo; inquirição, indagação, apuração*" (inquérito policial). Na esfera judiciária, a investigação diz respeito ao "*conjunto de atividades e diligências tomadas com o objetivo de esclarecer fatos ou situações de direito*", significado que será adotado no presente estudo (instrução probatória ou formação de provas).

Segundo Ferreira [5] (p. 1545), perícia é "*qualidade de perito; (...) habilidade, destreza; vistoria ou exame de caráter técnico e especializado (...) conjunto de peritos (ou um só) que faz essa vistoria (...) conhecimento, ciência*". Conforme Houaiss e Villar [4] (p. 2188), perícia é "*qualidade de perito; mestria (...) condição de quem é hábil; destreza (...) exame técnico de caráter especializado (...) a realização desse exame por perito(s); relatório referido por perito(s); laudo pericial (...) perito ou grupo de peritos que realiza esse exame (...) incidente do processo, relativo à prova, que consiste em confiar a um ou mais especialistas o encargo de fornecer ao juiz os elementos que lhe permitam tomar decisões*". A palavra perícia origina-se do latim *peritia* que significa conhecimento adquirido pelo uso, pela experiência. Perito também é uma palavra de origem latina (*peritu*), que significa pessoa provada no perigo, experimentada, especialista num ramo do saber (*expertus*). A perícia é uma atividade estritamente técnica e científica. Procura responder a questões específicas, utilizando métodos científicos, a respeito de um determinado fato. A perícia pode envolver a realização de exame ou vistoria (classes de perícia). Diniz [6] (p. 651) esclarece que "*exame é a apreciação de alguma coisa, por meio de peritos, para esclarecimento em juízo (...) vistoria é a mesma operação, porém restrita à inspeção ocular (...)*".

a) A Perícia no Escopo Judicial – Âmbito Civil

De acordo com o artigo 145, da Lei nº. 5.859, de 11/01/1973, Código de Processo Civil (CPC), "*quando a prova do fato depender de conhecimento técnico ou científico, o juiz será assistido por perito, segundo o disposto no art. 421*". Segundo o artigo 420, do CPC, "*a prova pericial consiste em exame, vistoria ou avaliação*". O parágrafo 1º., do artigo 145, do CPC, dispõe que "*os peritos serão escolhidos entre profissionais de nível universitário, devidamente inscritos no órgão de classe competente (…)*". Conforme o artigo 139, do CPC, "*são auxiliares do juízo, além de outros, cujas atribuições são determinadas pelas normas de organização judiciária, o escrivão, o oficial de justiça, o perito, o depositário, o administrador e o intérprete*". De acordo com o artigo 147, do CPC, "*o perito que, por dolo ou culpa, prestar informações inverídicas, responderá pelos prejuízos que causar à parte, ficará inabilitado, por 2 (dois) anos, a funcionar em outras perícias e incorrerá na sanção que a lei penal estabelecer*".Segundo o parágrafo 1º., do artigo 421, do CPC, "*incumbe às partes, dentro em 5 (cinco) dias, contados da intimação do despacho de nomeação do perito: I – indicar o assistente técnico; II – apresentar quesitos*". Conforme o artigo 429, do CPC, "*para o desempenho de sua função, podem o perito e os assistentes técnicos utilizar-se de todos os meios necessários, ouvindo testemunhas, obtendo informações, solicitando documentos que estejam em poder de parte ou em repartições públicas, bem como instruir o laudo com plantas, desenhos, fotografias e outras quaisquer peças*".

b) A Perícia no Escopo Judicial – Âmbito Penal

De acordo com o artigo 158, do Decreto-Lei nº. 3.689, de 03/10/1941, Código de Processo Penal (CPP), "*quando a infração deixar vestígios, será indispensável o exame de corpo de delito, direto ou indireto, não podendo supri-lo a confissão do acusado*". Segundo o artigo 159, do CPP, "*o exame de corpo de delito e outras perícias serão realizados por perito oficial, portador de diploma de curso superior*". O parágrafo 3º., do referido artigo, incluído pela lei nº. 11.690, de 09/06/2008, dispõe que "*serão facultadas ao Ministério Público, ao assistente de acusação, ao ofendido, ao querelante e ao acusado a formulação de quesitos e indicação de assistente técnico*". Conforme o artigo 169, do CPP, "*para o efeito de exame do local onde houver sido praticada a infração, a autoridade providenciará imediatamente para que não se altere o estado das coisas até a chegada dos peritos, que poderão instruir seus laudos com fotografias, desenhos ou esquemas elucidativos*". De acordo com o parágrafo único do referido artigo, "*os peritos registrarão, no laudo, as alterações do estado das coisas e discutirão, no relatório, as conseqüências dessas alterações na dinâmica dos fatos*".

3.2. O Processo de Investigação de Crimes Cibernéticos

a) A Fraude Informática e Evidência Eletrônica

Segundo o CERT-BR[1], citado por Pinheiro [7] (p. 264), "*a fraude eletrônica consiste em uma mensagem não solicitada que se passa por comunicação de uma instituição conhecida, como um banco, empresa ou site popular, e procura induzir usuários ao fornecimento de dados pessoais e financeiros*".

Segundo Porto [8] (p. 275), "*a fraude informática é uma modalidade da mais recente forma de manifestação delituosa, que é a chamada criminalidade informática, que compreende todas as lesões relacionadas com dados processados de maneira automática, sejam aquelas praticadas por meio do sistema informático ou da Internet, sejam aquelas praticadas contra os elementos lógicos do sistema, que são os dados e os programas dos computadores*".

De acordo com Pinheiro [7] (p. 180), "*a evidência de Digital é toda a informação ou assunto de criação/intervenção humana ou não, que pode ser extraído de um computador ou de outro dispositivo eletrônico*".

Para Pinheiro [7] (p. 182), "*(...) o escopo do exame forense é a extração de informações de qualquer vestígio relacionado com o caso investigado que permitam a formulação de conclusões acerca da infração. No universo da criminalística, vestígio é qualquer marca, fato, sinal ou material, que seja detectado em local onde haja sido praticado um fato delituoso*".

Segundo o artigo 239, do CPP, indício "*é a circunstância conhecida e provada, que, tendo relação com o fato, autorize, por indução, concluir-se a existência de outra ou outras circunstâncias*".

Pinheiro [7] (p. 185) aponta "*as cinco regras para a evidência eletrônica: – admissibilidade – deve ter condições de ser usada no processo – autenticidade – deve ser certa e de relevância para o caso – completa (no tunnel vision) – não*

[1] Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil.

pode causar ou levar a suspeitas alternativas – confiável – sem dúvidas sobre sua veracidade e autenticidade – possuir crédito (fazer acreditar) – clareza, fácil entendimento e interpretação".

b) Técnicas Forenses e Processo Forense

Ciência Forense é geralmente definida como a aplicação da ciência no Direito [9]. De acordo com Scudere [10] (p. 210), "*a ciência forense para computadores envolve a preservação, identificação, análise e estruturação de evidências armazenadas em computadores, na forma de informação magnética codificada (dados)*".

Conforme Pinheiro [7] (p. 182), "*a ciência forense busca desvendar cinco elementos: Quem?, O Quê?, Quando?, Como?, Onde? e Por quê?*".

De acordo com Kent et al. [11], "*técnicas forenses digitais envolvem a aplicação de ciência na identificação, coleta, exame e análise de dados de modo que preserve a integridade da informação e mantenha uma rigorosa cadeia de custódia para os dados*".

As técnicas forenses digitais podem ser usadas para muitos propósitos, tais como o apoio à investigação de crimes e violações de políticas internas, análises de incidentes de segurança, análises de problemas operacionais e recuperação de danos acidentais de sistemas [11]:

– Sistema Operacional: encontrar a localização virtual e física de um *host* com uma configuração de rede incorreta; resolver um problema funcional com uma aplicação; e registrar e rever o sistema operacional atual (SO) e as configurações de uma aplicação para um *host*.

– Monitoramento de *log*: analisar as entradas do *log* e as entradas a ele correlacionadas por meio de vários sistemas; auxiliar na investigação de incidentes; identificar violações de políticas; e auditoria e outros esforços relacionados.

– Recuperação de dados perdidos de sistemas, incluindo dados que foram acidentalmente ou propositalmente apagados ou modificados.

– Obtenção de dados para uso futuro de *hosts* que foram realocados ou aposentados: obtenção e armazenamento de dados de uma estação de trabalho de usuário quando o usuário deixa a organização. A *media* da estação de trabalho pode ser então preparada para a remoção de todos os dados originais do usuário.

– Proteção de informação sensitiva e manutenção de certos registros para fins de auditoria: habilita organizações para notificar outras agências ou indivíduos quando informação protegida é exposta a outras partes.

Para Scudere [10] (p. 214), "*os procedimentos típicos de um projeto de análise forense consistem em: a) identificação; b) coleta; c) preservação; e d) análise de informações digitais, visando atender os requisitos de evidências que podem ou não ser apresentados em juízo*".

Como adverte Corrêa [3] (p. 74), "*mesmo sabendo que quando um hacker invade determinado sistema pode esconder sua atividade por meio da desativação dos mecanismos de segurança, os arquivos sempre guardam o último horário em que foram acessados, os diretórios guardam uma espécie de "espelho" dos arquivos mesmo depois de terem sido apagados, e o disco rígido, na maioria das vezes, guarda informações dos arquivos apagados*".

Segundo Pinheiro [7] (p. 181), "*a computação forense consiste no uso de métodos científicos na preservação, coleta, validação, identificação, análise,*

interpretação, documentação e apresentação de evidência digital".

Kent et al. [11] descrevem um processo de quatro passos para a aplicação de técnicas forenses digitais de um modo consistente:

– **Coleta.** O dado é identificado, rotulado, registrado e capturado de todas as fontes possíveis de dados relevantes, usando procedimentos que preservam a integridade do dado. O dado deveria ser coletado de um modo antecipado para impedir a perda de dados dinâmicos, tais como uma lista de conexões de rede atuais, e os dados coletados em telefones celulares, *PDAs* e outros dispositivos alimentados por baterias.

– **Exame.** O dado que é coletado deveria ser examinado usando uma combinação de métodos automáticos e manuais para avaliar e extrair dados de interesse particular para uma situação específica, enquanto preserva a integridade do dado.

– **Análise.** Os resultados do exame deveriam ser analisados, usando métodos e técnicas bem documentados, para derivar informação útil que endereça as questões que foram a motivação para a coleta e o exame.

– **Relatório.** Os resultados da análise deveriam ser relatados. Os itens que serão relatados podem incluir: a descrição das ações tomadas; a explanação de como as ferramentas e os procedimentos foram selecionados; a determinação de qualquer outra ação que deveria ser desenvolvida, tais como exame forense de fontes de dados adicionais, vulnerabilidades de segurança identificadas, e melhoria dos controles de segurança existentes. E recomendações para melhorias de políticas, guias, procedimentos, ferramentas, e outros aspectos do processo forense.

3.3. Ciclos de Vida de Desenvolvimento de Sistemas de Informação.

Existem na literatura vários estudos sobre os ciclos de vida de desenvolvimento de sistemas de informação (CVDSs), entre os quais encontram-se os trabalhos de Pressman [12], Blum [13], Yourdon [14] e Senn [15].

Não há uniformidade para definir e descrever o ciclo de vida de um sistema de informação. Algumas vezes, diferentes ciclos de desenvolvimento são definidos com base na estratégia de desenvolvimento [12,16, 17,18].

Entre os principais paradigmas para o desenvolvimento de projetos de sistemas de informação apresentados pela literatura estão o modelo seqüencial linear [14,15], o modelo de prototipagem [12,14], o modelo RAD [12] e os modelos evolucionários – modelo incremental, modelo espiral e modelo baseado em componentes [12,19].

3.4. Adoção de Técnicas Forenses pelos CVDSs

De acordo com Kissel et al. [20], as seguintes técnicas deveriam ser adotadas pelos ciclos de vida de desenvolvimento de sistemas de informação: realização regular de *backups* de sistemas e manutenção de *backups* anteriores por um determinado período de tempo; auditoria em estações-de-trabalho, servidores e dispositivos de rede; transferência de registros de auditoria para servidores de *log* centralizados; configuração de aplicações *mission-critical* para desenvolver auditoria, incluindo registro de todos os acessos autenticados; manutenção de um banco de dados de arquivos *hashes* para arquivos comuns de SO e aplicações; uso de software de verificação da integridade em ativos

importantes; manutenção de registros de configurações de rede e de sistema; estabelecimento de políticas de retenção de dados que suportam o desenvolvimento de revisões históricas de atividades de sistema e de rede, de acordo com as solicitações e requisitos para preservar dados relativos a litigações e investigações e destruição de dados que não mais interessam.

4. Metodologia

Para Lakatos e Marconi [21], "*a finalidade da atividade cientifica é a obtenção da verdade, por intermédio da comprovação de hipóteses, que, por sua vez, são pontes entre a observação da realidade e a teoria cientifica, que explica a realidade*". Dentre as alternativas metodológicas – pesquisas descritivas, pesquisas explicativas e pesquisas exploratórias – optou-se pela pesquisa exploratória [22,23]. "*Em geral, (…) questões do tipo "Como" e "Por quê" são mais favorecidas pelo uso de estudos de caso, experimentos ou histórias*" [22].

A presente pesquisa tem por objetivo responder a questões do tipo "Como", o que conduz ao estudo de caso. Desse modo, para analisar o processo de investigação de crimes cometidos no ambiente da Tecnologia da Informação, levantando as técnicas forenses adotadas pelos ciclos de vida de desenvolvimento de sistemas de informação, a metodologia utilizada foi o estudo de casos múltiplos, o que permitiu ao pesquisador o aprofundamento em alguns aspectos do processo de investigação de crime cibernéticos [22,24,25,26]. Com base no que foi discutido anteriormente e para obter os dados para este estudo, foi selecionada uma amostra de caráter intencional – por julgamento ou não-probabilística – por ser possível identificar e entrevistar elementos definidos da população [21,27,28], formada por seis instituições financeiras (IFs). Após a seleção das instituições financeiras pesquisadas, foram realizadas entrevistas com os gerentes dos centros de desenvolvimento de sistemas de informação dessas instituições, responsáveis pelo ciclo de desenvolvimento de sistemas adotado pela instituição. Muito embora a generalização dos resultados não possa ser realizada devido à natureza da amostra não ser probabilística, espera-se que este modelo de pesquisa permita obter resultados que tenham validade no contexto da amostra selecionada e que possam ser comparados com pesquisas anteriores sobre o tema.

Considerando os objetivos da presente pesquisa, a forma de coleta de dados adotada foi a de observação direta intensiva, com a utilização da técnica de entrevista, do tipo padronizada ou estruturada, segundo o roteiro e o formulário previamente elaborados, complementada, quando possível, com consultas a material referente ao ciclo de vida de desenvolvimento de sistemas [21].

5. Análise dos resultados

Com base nas entrevistas e observações realizada pelo pesquisador, pode-se constatar que a adoção de um CVDS é obrigatória em todas as instituições financeiras, independentemente da origem do capital, do porte da instituição financeira e da equipe de desenvolvimento. Pode-se verificar que, embora possam adotar outros ciclos de vida de desenvolvimento de sistemas abordados em sua metodologia [13], todas as instituições financeiras adotam o

modelo seqüencial linear e o modelo baseado em componentes, o que demonstra que o ciclo de vida clássico continua sendo o mais amplamente utilizado [12,17]. Cabe observar que nessas instituições financeiras a maior parte dos projetos de sistemas de informação é desenvolvida por equipes mistas (formadas por funcionários e contratados), ou seja, é desenvolvida internamente. Pode-se verificar que, quando isso ocorre, existe mais rigor na adoção de um determinado CVDS pela instituição financeira.

Por sua vez, durante a pesquisa realizada junto às instituições financeiras selecionadas, foi observada a adoção de processos para gerenciamento do risco, abordando criptografia e outras técnicas e ferramentas com o objetivo de identificar, avaliar, planejar a resposta e controlar e monitorar o evento de risco.

Uma vez analisados os ciclos de vida de desenvolvimento de sistemas de informação e os processos para gerenciamento do risco adotados pelas instituições financeiras pesquisadas, pode-se verificar quais técnicas forenses são adotadas. Os resultados obtidos estão apresentados no Quadro 1:

Técnicas Forenses	IF #01	IF #02	IF #03	IF #04	IF #05	IF #06
Sistema Operacional	Não	Não	Sim	Sim	Não	Não
Monitoramento de *log*	Sim	Sim	Sim	Sim	Sim	Sim
Recuperação de dados	Sim	Sim	Sim	Sim	Não	Não
Obtenção de dados	Não	Não	Sim	Sim	Não	Não
Proteção de informação	Não	Não	Sim	Sim	Não	Não

Quadro 1 – Adoção de técnicas forenses pelos CVDSs por instituição financeira

Pode-se verificar que, nas instituições financeiras de grande porte e capital nacional (IF #01 e IF #02), existem políticas e recomendações que orientam o processo de planejamento da resposta ao risco. Todavia, das técnicas forenses que permitiriam a coleta, exame, análise e relatório, como propõe Kent et al. [11], após a ocorrência do evento de risco, foi observada a adoção de apenas duas delas.

Pode-se constatar, ainda, que nas instituições financeiras de médio porte e capital internacional (IF #03 e IF #04), existem políticas e recomendações originadas da própria matriz, o que revela a sua influência no processo de planejamento da resposta ao risco. Por conseqüência, todas as técnicas forenses apontadas são adotadas.

Nas instituições financeiras de pequeno porte (IF #05 e IF #06), não existe uma regra específica para esse processo, indicando que, nessas instituições financeiras, o processo de planejamento da resposta ao risco ainda é muito incipiente, sequer foi sistematizado. Conseqüentemente, das técnicas forenses apontadas por Kent et al. [11] e Kissel et al. [20], apenas uma é adotada, o que pode dificultar o processo de investigação quando da ocorrência de eventual fraude.

Por fim, em nenhuma das instituições financeiras pesquisadas foram identificadas políticas e recomendações específicas para o processo de investigação de crimes cibernéticos.

6. Conclusões

A pesquisa exploratória procurou analisar a aplicação da ciência forense à

Tecnologia da Informação. Como se pode constatar, o presente estudo revelou a necessidade de adoção de técnicas forenses pelos ciclos de vida de desenvolvimento de sistemas de informação, o que permitiria aumentar a eficácia e a eficiência do processo de investigação de eventuais fraudes.

Como o estudo foi baseado em amostra intencional, torna-se limitada a possibilidade de realizar generalizações sobre as conclusões do trabalho. Porém, pelas instituições financeiras pesquisadas, é possível afirmar que os ciclos de vida de desenvolvimento de sistemas de informação estudados nesta pesquisa são bastante representativos do universo da população.

Deste modo, o objetivo do presente trabalho foi atingido durante seu desenvolvimento, com base nas entrevistas realizadas. Foi possível contrapor os aspectos pertinentes à ciência forense com o ambiente de Tecnologia da Informação.

Pela avaliação das técnicas forenses, este artigo não apenas poderá auxiliar em sua implementação pelos ciclos de vida de desenvolvimento de sistemas de informação, como também poderá contribuir para aumentar a eficácia e eficiência do processo de investigação de crimes cibernéticos.

Referências Bibliográficas

[1] WALD, Arnold (2001), Um novo direito para a nova economia: os contratos eletrônicos e o Código Civil. In: GRECO, Marco Aurélio; MARTINS, Ives Gandra (coordenadores). *Direito e Internet: relações jurídicas na sociedade informatizada*. São Paulo: Editora Revista dos Tribunais. Cap. 1.

[2] OLIVEIRA, Mauricio Lopes de (2002), Seis propostas para o ciberespaço. In: FILHO, Valdir de Oliveira Rocha; BARRETO, Ana Carolina Horta (coordenadores) et al. *O direito e a internet*. Rio de Janeiro: Forense Universitária.

[3] CORRËA, Gustavo Testa (2007), *Aspectos Jurídicos da Internet*. 3ª. Ed. São Paulo: Editora Saraiva.

[4] HOUAISS, Antönio, VILLAR, Mauro de Salles (2001), *Dicionário Houaiss da língua portuguesa*. Rio de Janeiro: Objetiva.

[5] FERREIRA, Aurélio Buarque de Holanda (1999), *Novo Aurélio século XXI*: o dicionário da língua portuguesa. 3ª. Ed. Rio de Janeiro: Nova Fronteira.

[6] DINIZ, Maria Helena (2005), *Dicionário jurídico*. Vol. 3. 2ª. Ed. São Paulo: Saraiva.

[7] PINHEIRO, Patrícia Peck (2007), *Direito digital*. 2ª. Ed. São Paulo: Editora Saraiva.

[8] PORTO, Luiz Guilherme Moreira (2001), Fraude Informática. In: SILVA JUNIOR, Ronaldo Lemos da; WAISBERG, Ivo. *Comércio eletrônico*. São Paulo: Editora Revista dos Tribunais. Cap. 11.

[9] RADACK, Shirley (2009), Forensic techniques: helping organizations improve their responses to information security incidents. Disponível em http://www.itl.nist.gov/lab/bulletns/bltnsep06.htm. Acesso em 06 jul.

[10] SCUDERE, Leonardo (2006), Análise Forense – Tecnologia. In: BLUM, Renato M. S. Opice; BRUNO, Marcos Homes da Silva e ABRUSIO, Juliana Canha (coordenadores). *Manual de direito: eletrônico e Internet*. São Paulo: Lex Editora. Cap. 13.

[11] KENT, Karen, CHEVALIER, Suzanne, GRANCE, Tim, DANG, Hung (2006), *Guide to integrating forensic techniques into incident response*: recommendations

of the National Institute of Standards and Technology. Special Publication 800-86. Gaithersburg, MD: NIST.
[12] PRESSMAN, Roger S. (2002), *Engenharia de Software*. 5ª. Ed. São Paulo: McGrawHill.
[13] BLUM, Bruce I. (1994), A taxonomy of software development methods. *Communications of ACM*, New York, v. 37, n. 11, p. 82-94, Nov.
[14] YOURDON, Edward (1989). *Modern Structured Analysis*. Englewood Cliffs: Yourdon Press.
[15] SENN, James A. (1989), *Analysis and design of information systems*. 2ª. Ed. New York: McGraw-Hill, 1989.
[16] APPLEGATE, Lynda M., AUSTIN, Robert D. e MCFARLAN, F. Warren (2003), *Corporate information strategy and management:* the challenges of managing in a network economy. 6a. Ed. New York: McGraw Hill.
[17] GREEN, Darryl e DICATERINO, Ann (2004), A survey of system development process models. Albany: Center for Technology in Government, 1998. Disponível em <http://www.ctg.albany.edu/publications/reports/survey_of_sysdev/survey_of_sysdev.pdf> Acesso em 5 jan.
[18] CLELAND, David I. e KING, William R. (1983), *Project management handbook*. New York: Van Nostrand Reinhold.
[19] BOEHM, Barry W. (1988), A spiral model of software development and enhancement. *IEEE Computer,* p. 61-72, May .
[20] KISSEL, Richard, STINE, Kevin, SCHOLL, Matthew, ROSSMAN, Hart, FAHLSING, Jim, GULICK, Jéssica (2008), *Security considerations in the system development life cycle*. Special Publication 800-64 Revision 2. Gaithersburg, MD: NIST.
[21] LAKATOS, Eva Maria. MARCONI, Marina de Andrade (2000), *Metodologia Cientifica*. 3ª. Ed. São Paulo: Atlas.
[22] YIN, R. K. (1999), *Case study research*: design and methods. 6ª. ed. Thousand Oaks: SAGE Publications, Inc.
[23] NOGUEIRA, Oracy (1968), *Pesquisa social:* introdução às suas técnicas. São Paulo: Nacional, EDUSP, apud LAKATOS, Eva Maria e MARCONI, Marina de Andrade (1991), *Fundamentos de metodologia científica*. 3ª. Ed. São Paulo: Atlas.
[24] LAVILLE, Christian e DIONNE, Jean (1999), *A construção do saber:* manual de metodologia da pesquisa em ciências humanas. Porto Alegre: Artes Médicas Sul.
[25] COOK, Thomas D. e REICHARDT, Charles S. (1979), *Qualitative and quantitative methods in evaluation research*. Beverly Hills: Sarge.
[26] SCHRAMM, W. (1971), *Notes on case studies of instructional media projects*. Working paper, the Academy for Educational Development, Washington, Dec., apud TACHIZAWA, T. (2002), *Metodologia da pesquisa aplicada à administração:* a internet como instrumento de pesquisa. Rio de Janeiro: Pontal.
[27] CASTRO, Claudio de Moura (2006), *A prática da pesquisa.* São Paulo: Prentice-Hall.
[28] MATTAR, Fauze Najib (1993). *Pesquisa de Marketing*. São Paulo: Atlas.

Anexo 1 – Formulário para a entrevista

Parte I – Caracterização da instituição financeira.

1. Produto(s) e serviço(s) oferecido(s):

□ Conta corrente.
□ Investimentos.
□ Empréstimos.
□ Financiamentos.
□ Crédito Pessoal.
□ Cartão de Crédito.
□ Crédito Direto ao Consumidor.
□ Crédito Imobiliário.
□ Consórcios.
□ Cobrança.
□ Seguros.
□ Capitalização.
□ Previdência Privada.
□ Administração de Recursos de Terceiros.
□ Câmbio.
□ Comércio Exterior.
□ Outro.

2. Tipo(s) de acesso disponibilizado(s) aos clientes:

□ Agências.
□ Postos de atendimento bancário (PABs).
□ Agências em *store-banking*.
□ Lojas de financiamento.
□ Máquinas de auto-atendimento.
□ Quiosques.
□ Serviço Telefônico.
□ *Internet banking*.
□ Outro.

3. Origem do capital:

□ Nacional.
□ Internacional.
□ Misto.

4. Valor total do ativo (R$ mil):

□ Menos de 10.000.000.
□ Entre 10.000.000 e 20.000.000.
□ Mais de 20.000.000.

5. Número de funcionários na área de TI (tempo integral, ou seja, 8 horas/dia):

□ menos de 1000.
□ entre 1000 e 2000.
□ mais de 2000.

6. Número de contratados na área de TI (tempo integral, ou seja, 8 horas/dia):

□ menos de 1000.
□ entre 1000 e 2000.
□ mais de 2000.

Parte II – Caracterização da prática de projetos de sistemas de informação.

7. Identificar o(s) Ciclo(s) de Vida de Desenvolvimento de Sistemas adotado(s) pela instituição financeira:

□ Modelo Seqüencial Linear.
□ Modelo de Prototipagem.
□ Modelo RAD.
□ Modelo Incremental.
□ Modelo Espiral.
□ Modelo Baseado em Componentes.
□ Outro (especificar):

8. Identificar a(s) técnica(s) forense(s) requerida(s) pelo(s) Ciclo(s) de Vida de Desenvolvimento de Sistemas adotado(s) pela instituição financeira:

□ Sistema Operacional: encontrar a localização virtual e física de um *host* com uma configuração de rede incorreta; resolver um problema funcional com uma aplicação; e registrar e rever o sistema operacional atual (SO) e as configurações de uma aplicação para um *host*.
□ Monitoramento de *log*: analisar as entradas do *log* e as entradas a ele correlacionadas por

meio de vários sistemas; auxiliar na investigação de incidentes; identificar violações de políticas; e auditoria e outros esforços relacionados.

□ Recuperação de dados perdidos de sistemas, incluindo dados que foram acidentalmente ou propositalmente apagados ou modificados.

□ Obtenção de dados para uso futuro de *hosts* que foram realocados ou aposentados: obtenção e armazenamento de dados de uma estação de trabalho de usuário quando o usuário deixa a organização. A *media* da estação de trabalho pode ser então preparada para a remoção de todos os dados originais do usuário.

□ Proteção de informação sensitiva e manutenção de certos registros para fins de auditoria: habilita organizações para notificar outras agências ou indivíduos quando informação protegida é exposta a outras partes.

9. Verificar qual/quais é/são a(s) regra(s) / política (s) aplicável/aplicáveis ao processo de investigação de fraude(s), caso exista(m).

Parte III – Caracterização do processo de planejamento da resposta ao risco.

10. Identificar em que categoria(s) de projetos de sistemas de informação o processo de planejamento da resposta ao risco deve ser adotado:

Equipe de desenvolvimento:

□ Exclusivamente interna (apenas funcionários).
□ Mista (funcionários e contratados)
□ Exclusivamente externa (apenas contratados).

Custo total do projeto (em R$ mil):

□ Menor que 100.
□ Entre 100 e 500.
□ Entre 500 e 1.000.
□ Entre 1.000 e 2.000.
□ Maior que 2.000.

Prazo total do projeto (em meses):

□ Menor que 6.
□ Entre 6 e 12.
□ Entre 12 e 18.
□ Entre 18 e 24.
□ Maior que 24.

Esforço total do projeto (em homens-hora):

□ Menor que 10.000.
□ Entre 10.000 e 50.000.
□ Maior que 50.000.

11. Identificar a(s) técnica(s) / ferramenta(s) utilizada(s) no processo de planejamento da resposta ao risco adotado pela instituição financeira:

12. Verificar qual/quais é/são a(s) regra(s) / política (s) aplicável/aplicáveis ao processo de planejamento da resposta ao risco, caso exista(m).

Contato

R. Doutor Brasílio Machado, 267 – apto. 31 – Santa Cecília – CEP 01230-010 – São Paulo – SP
Fone residencial: (11) 3666-0633/Celular: (11) 9798-8567