Modelo de gestão de incidentes de fraude via sistemas de informação

Luciana Cantarelli [a], Ananias Queiroga [b]

***Abstract*—It is common to see information systems incorporating critical functionalities and the increasing number of people who uses it as a working tool. For this reason, precautions need to be taken to avoid fraud via these systems. In case the fraud is detected, it is important to recognize the way to perform the investigation to search for the author. A legally valid investigation must follow proceedings recognized by computer forensics science. The mitigation of fraud risk, in the other hand, can be reached by an effective information technology governance and acceptance of good practices recommendations. Therefore, in this paper, we propose a method to manage incidents of fraud respecting good practices of cybercrime investigation and TI governance.**

***Keywords*—Computação Forense; Fraude; Governança de TI; Processo de Investigação.**

1. Introdução

A transmissão e a comunicação de informações nas empresas e suas áreas de negócio estão cada vez mais suportadas por sistemas de informação. Operações como transferência de fundos, emissão de pedidos e de nota fiscais são exemplos de rotinas já incorporadas pelos sistemas corporativos. Não obstante a esta realidade, é comum encontrar empresas vítimas de fraudes realizadas através de seus próprios sistemas e falta de preparado dos gestores para condução e tratamentos desses tipos de ocorrência. Os registros de incidentes relacionados à fraude reportados ao CERT.br (Centro de Estudo, Resposta e Tratamento de Incidentes no Brasil) mostram um aumento de 61% de 2008 para 2009. No primeiro quadrimestre de 2010 já existem 28325 ocorrências, praticamente o mesmo reportado durante todo o ano de 2002.

A auditoria e consultoria, KPMG, publicou uma pesquisa realizada em 2008 com executivos seniores de 204 empresas americanas com faturamento superior a US$ 250 milhões. Nesta pesquisa, foi identificado que 65% dos executivos consideram a fraude um risco significante; 35% consideram a apropriação indevida de ativos como a fraude mais preocupante; 71% consideram o dano à imagem e reputação a pior conseqüência de uma fraude; e 66% consideram que as fraudes ocorrem devido às falhas e/ou falta de controles internos.

Ao que se refere ao tratamento das ocorrências de fraude, 20% reconhecem não saber quem deve conduzir a investigação; 27% não sabem como realizar uma investigação; e 27% não sabem quando a mesa diretora deve tomar conhecimento da fraude. Esse resultado mostra a relevância de se ter um conhecimento consistente e aprofundado acerca do tema.

Este trabalho tem como objetivo propor um modelo de gestão de incidentes de fraude que integre as boas práticas do processo de investigação e de correção de erros, trazendo como resultado menores perdas, maiores chances de recuperação pecuniária e de identificação/punição dos culpados.

2. Governança Corporativa e Sistema de Informação

A governança empresarial é uma forma de estabelecer normas e padrões para evitar e lidar com as fraudes nas organizações. O Committee of Sponsoring Organizations, COSO, fundado em 1985, respaldou esta visão e é reconhecido por prover diretrizes e aspectos críticos de governança organizacional através da ética empresarial e controles internos a fim de produzir meios impeditivos para ocorrência e correção dos danos causados pelo mau uso das ferramentas administrativas.

Os delitos de fraude relacionados à Tecnologia da Informação (TI) são classificados em virtuais puros, mistos e comuns [1]. A fraude virtual pura é o ilícito contra o computador (sistema e equipamento). A fraude virtual mista seria aquela que o dolo é realizado por meio da informática, porém visa atingir outros bens. A fraude virtual comum é aquela que já é encontrada na forma de lei uma tipificação penal.

A fim de lidar de maneira mais eficaz com os incidentes, as empresas passaram a utilizar frameworks de governança de TI. Neste artigo seguiremos as recomendações do framework, Cobit 4.1, que estão organizadas em quatro domínios. O primeiro é Planejamento e Organização (PO) que cobre o plano estratégico e tático e se preocupa com o modo que a TI pode melhor contribui para o atendimento dos objetivos do negócio. O segundo domínio, Adquirir e Implementar (AI), trata da identificação, desenvolvimento e aquisição de soluções de TI aderente às estratégias de TI. O terceiro domínio, Entrega e Suporte (ES), preocupa-se com o nível de entrega dos serviços, gestão de segurança, continuidade, suporte aos usuários e gestão de recursos de dados e equipamentos. O quarto e último domínio, Monitorar e Avaliar (MA), recomenda que todos os processos de TI devam ser regularmente avaliados em relação à qualidade e adequação às normas corporativas.

3. Computação Forense no Controle de Fraudes

Apesar de apresentar grandes avanços, o Cobit ainda se mostra pouco efetivo na identificação e correção de erros do e no sistema, nos casos de fraude. A literatura apoiada em diversas pesquisas tais como Neukamp [2], Oliveira [3], Noblett, Pollitt & Presley [4], Reis [5] e Toscano [6] demonstra que o sistema de governança corporativa se torna mais eficiente na gestão de incidentes de fraude com a utilização combinada de princípios de controle administrativo e premissas da ciência forense computacional.

Forense computacional pode ser definida como a área da criminalística que abarca a aquisição, prevenção, restauração e análise de evidências computacionais, onde podem ser objetos físicos, informações trabalhadas eletronicamente ou arquivados em meios computacionais [7] [8]. Este entendimento fornece uma ampla base de suporte para a gestão de fraudes.

O emprego da forense computacional dentro das empresas agrega competências técnicas e fornece instrumentos que tornam as organizações mais capazes e eficientes no combate à fraude [6]. Os procedimentos de investigação forense necessitam ter um elevado padrão de condição de qualidade com a finalidade de salvaguardar a credibilidade e a exatidão de possíveis provas e registros. A fig 1 é um modelo hierárquico multidimensional para visualização da forense computacional [9] e denota uma grande aplicabilidade dentro das empresas, pois a estrutura respeita diversos modelos de gestão tradicionalmente utilizados e está adequado a concepção de auditoria interna moderna [1] [10].

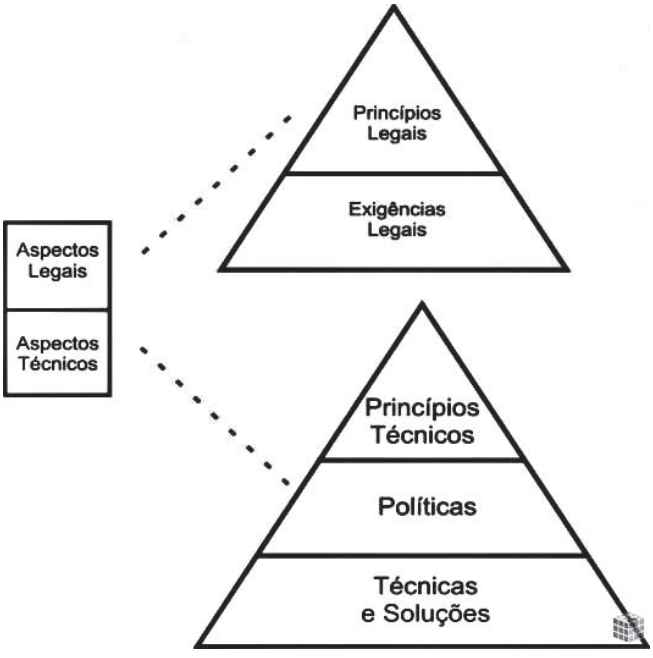

Fig. 1 Modelo hierárquico da forense computacional.

Portanto, obter e conservar de forma adequada as evidências é condição basilar para uma prática eficaz do tratamento dos incidentes de fraude e validade dos instrumentos de controle interno das empresas. Para alcançar esta maturidade, as empresas devem ter a preocupação prévia ao incidente, com o uso pertinente da tecnologia, construindo, assim, alicerce seguro para uma investigação e mitigando os impactos da ocorrência de fraudes [6].

4. Gestão para Incidentes de Fraudes

Utilizando as melhores práticas de investigação de crime cibernético e de governança de TI, os autores elaboraram uma visão gerencial para o tratamento de casos de fraude realizada através de sistemas de informação. Esses sistemas usualmente possuem controles de acesso onde os usuários são identificados, autenticados e autorizados a executar funções, acarretando particulares impactos no âmbito financeiro [10].

O controle de acesso é eficaz para a identificação da autoria de uma fraude, mas pode ser facilmente fragilizado, como das seguintes formas [10] [9]:

- Roubo, adivinhação e compartilhamento de senha de acesso entre os usuários;
- Erro na concessão e manutenção do perfil de acesso; e
- Falha na desabilitação de usuário que não mais compõe o corpo organizacional.

Para que seja identificada a origem e autoria da fraude via sistemas de informação, é importante determinar o terminal de computador que partiu os comandos fraudulentos e o usuário deste computador no momento da execução das operações. É comum que os endereços dos terminais (IP) em uma rede computador sejam alocados dinamicamente, ou seja, os endereços dos terminais podem ser alterados ao sabor do protocolo de configuração dinâmica de computadores (DHCP) e sem a intervenção do gestor da rede. Esta configuração pode prejudicar o rastreamento dos terminais de onde partiram os comandos fraudulentos, caso seja o IP a informação registrada em log [8]. Não é o intuito desde artigo propor uma orientação técnica de métodos para localizar fisicamente os terminais de computadores dentro da organização.

Questão fundamental para a gestão dos incidentes de fraude é enfrentar e conciliar os desdobramentos legais e administrativos após a identificação da fraude. A fig. 2 ilustra uma cronologia de fases que deve ser consideradas pela gestão de incidente de fraude.

Fig. 2. Linha de tempo e a relação entre os esforços de governança, duração da fraude, processo investigativo e correção de erros.

Além da identificação interna do autor e das medidas administrativas tomadas pelo gestor de incidente, pode

ocorrer, a depender da decisão da organização, o envolvimento da polícia para buscar punição dos responsáveis pela fraude. Caso a organização decida por instaurar um boletim de ocorrência policial, a organização deve tomar precauções para que as evidências não percam seu valor como prova material. É importante salientar que mesmo que o processo investigativo seja realizado por perito designado por juiz de direito para análise do caso, é necessário conhecer a cadeia de custódia do departamento policial que irá investigar a fraude para entender como as conclusões são alcançadas e manter a validade legal das evidências digitais geradas durante a ocorrência da fraude [11].

Em momento apropriado, durante ou após o processo de investigação, a organização deve fazer um levantamento de suas práticas de governança e identificar os pontos fracos ou as falhas de procedimentos, dando início, assim, a um trabalho de correção de erros. Devido à natureza evolutiva dos casos de fraude, a revisão periódica nos controles internos e procedimentos são necessários para manter o risco e impactos da fraude em patamares menores e de rápida detecção e tratamento [5].

A ocorrência de fraudes em um sistema de informação deve ser analisada com base em uma avaliação do ambiente [5], buscando ponderar e entende-lo como permissivo ou impeditivo para o surgimento de fraudes. Ademais, esta verificação é que permitirá a definição de prioridades respeitando as características de cada caso e empresa.

Um ambiente permissivo aqui definido como local ou circunstância onde há demasiada tolerância a comportamentos e procedimentos propensos a condutas fraudulentas. Sendo a fraude identificada em ambiente permissivo, deve-se priorizar as correções dos erros, pois é fundamental sanar as distorções que tornam o ambiente uma fonte facilitadora de fraudes. As correcões visam evitar reinicidência e prejuízos maiores às organizações e colaborar para que uma possível investigação transcorra com base em dados seguros.

Por ambiente impeditivo compreende-se um espaço que iniba e dificulte a ação de atos fraudulentos, procurando impossibilitar de maneira preventiva que as fraudes ocorram, entretanto, havendo alguma mínima incidência que essa seja de rápida identificação e de menor impacto. Nesta forma de ambiente, quando da existência de fraude, o foco central a ser delineado pela administração é o da investigação, evidenciando-se a necessidade de encontrar o fraudador. O ambiente impeditivo, em si, já é um modelo de controle que facilita a correção de erros, sendo assim, um arcabouço de dados precisos e seguros para uma investigação.

Em qualquer que seja o ambiente, a comunicação entre o gestor responsável pela resposta ao incidente de fraude e a liderança deve ser feita periodicamente ao longo do processo investigativo e de correção de erros, a fim de manter a alta administração ciente dos resultados dos esforços e compartilhar as tomadas de decisão [10].

4.1 Modelo de Gestão de Incidentes de Fraudes

Seguindo as duas linhas de atuação, investigação e correção de erros, propomos um modelo de gestão de incidentes de fraudes que procura unir as práticas da computação forense com as de governança de TI, de forma a orientar como o gerente responsável pela resposta ao incidente deve conduzir de forma macro todo esse processo.

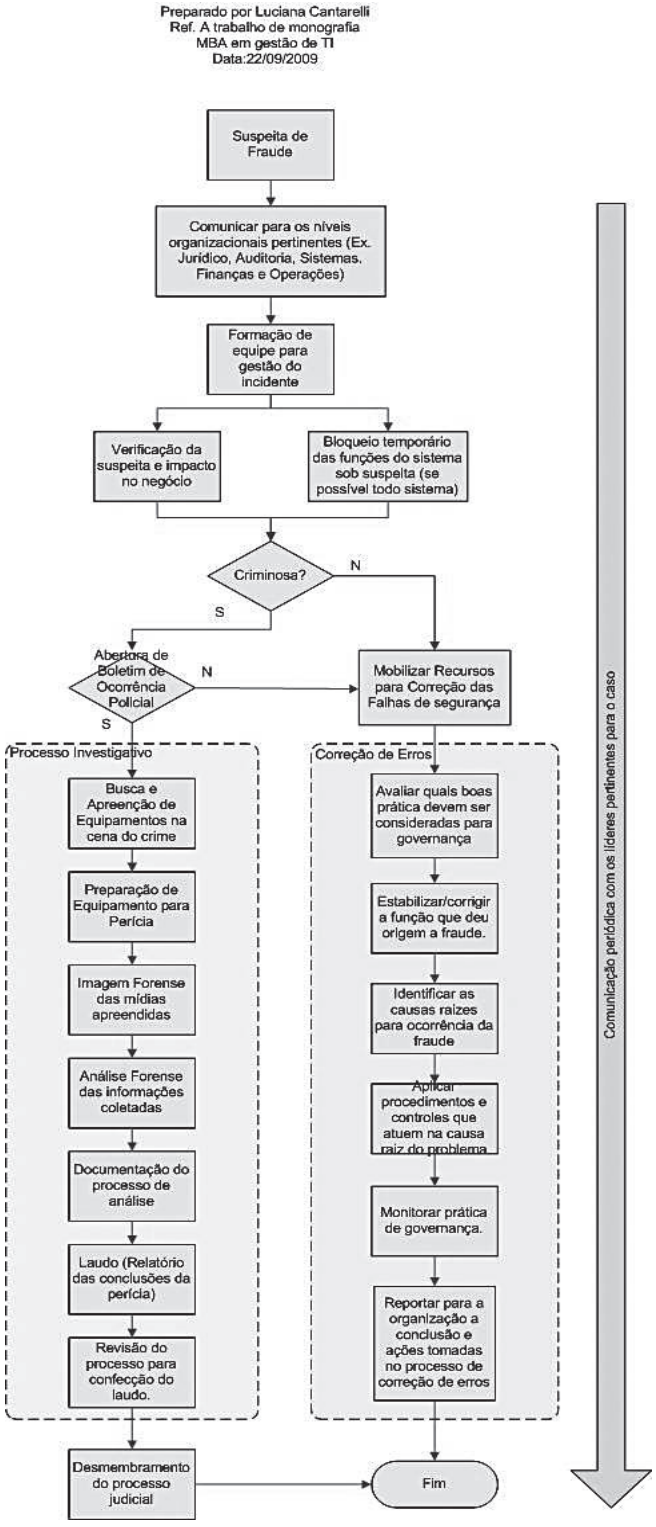

Fig. 3. Modelo de gestão de incidentes de fraudes.

A proposta ilustrada tem o objetivo de mostrar quais etapas e procedimentos precisam ser considerados pela organização, na função do Gestor de Resposta a Incidente de Fraude, para minimizar as perdas, aumentar as chances de recuperação do montante furtado, identificar e punir na forma da lei os culpados. No entanto, esta não é fórmula estática, mas se propõe uma compreensão dinâmica, pois cada organização deve se posicionar no processo de resposta aos incidentes de fraude, indicando elementos que estejam em acordo com suas normais internas e experiências vividas.

5. Conclusão

Com a elaboração desse trabalho foi proposto um modelo de gestão de incidentes de fraudes em um ambiente corporativo, usando como base as boas práticas recomendadas pelo grupo de trabalho científico em evidência digital, SWGDE, e o modelo prático de governança de tecnologia da informação, Cobit. Chamamos de Gestor de Resposta a Incidente de Fraude a pessoa designada pela organização para coordenar as tomadas de decisão após a identificação de suspeita da fraude. A velocidade e a qualidade de suas ações, portanto, tem reflexos no processo investigativo e de correção de erros.

Aqui foi apresentado um modelo gerencial de boas práticas em computação forense para que o gestor de resposta ao incidente tenha o conhecimento necessário sobre o processo investigativo seguido por departamentos policiais, já que os computadores utilizados são considerados elementos fundamentais da cena do crime. Qualquer modificação no conteúdo ou na forma dos dados armazenados nesses computadores pode impugnar as evidências de autoria da fraude, deste modo, faz-se necessário rigor nas práticas de computação forense para preservação dos dados contidos nesses ambientes.

Ao passo que o processo investigativo criminal é realizado pela perícia técnica designado para o caso, o Gestor de Resposta ao Incidente deve compreender quais controles são recomendados para aumentar o nível de maturidade da governança em seu ambiente de tecnologia, para corrigir os erros e manter um elevado nível de segurança da informação no ambiente computacional da empresa.

O Gestor de Resposta ao Incidente, portanto, deve ser considerado o elo entre as decisões estratégicas e táticas para resolução do incidente; salvaguardando as evidências digitais; sendo responsável pela implementação de medidas corretivas; e funcionar como via de comunicação acerca do status da ocorrência para a organização.

Em relação o ambiente onde a fraude ocorreu, podemos complementar que o nível de esforço nas frentes de investigação e correção de erros dependerá da qualidade dos controles internos. Se o ambiente for permissivo, ou seja, existir uma predisposição para ocorrência de fraude, o trabalho para correção de erro será muito mais intenso ao passo que deve existir poucas evidências para conclusão de um processo investigativo. Na outra mão, existem os ambientes impeditivos que são os que possuem bons controles internos, inibem a ocorrência de fraudes e facilitam o processo de investigação. Nesse caso, o processo de investigação se estabelece como o mais relevante devido à quantidade e qualidades das evidências geradas durante a fraude.

Referências

[1] J. M. S. Pinheiro. Auditoria e Análise de Segurança da Informação: Forense Computacional. UGB, 2009.

[2] P. A. Neukamp. Forense Computacional: Fundamentos e Desafios Atuais. Universidade do Vale do Rio dos Sinos (UNISINOS), 2007.

[3] F. S. Oliveira. Resposta a Incidentes e Analise Forense Para Redes Baseadas em Windows 2000. Dissertação (Mestrado em Ciência da Computação) – Instituto de Computação, Universidade Estadual de Campinas, 2002.

[4] M. G. Noblett, M. M. Pollitt and L. A. Presley. Recovering and Examining Computer Forensic Evidence. Forense Science Communications. Vol. 2 N. 4; Federal Bureau of Investigation, 2000.

[5] M. A. Reis. Forense computacional e sua aplicação em segurança imunológica. Dissertação (Mestrado em Ciência da Computação) – Instituto de Computação, Universidade Estadual de Campinas, 2003.

[6] W. Toscano. Auditoria Forense Computacional: Introdução. USP, São Paulo, 2009.

[7] A. R. Freitas. Perícia Forense Aplicada à Informática: Ambiente Microsoft. Rio de Janeiro: Brasport, 2006.

[8] B. CARRIER and J. Grand. A Hardware-Based Memory Acquisition Procedure For Digital Investigations. Digital Investigation Journal, 2004.

[9] H. C. Ulbrich and J. D. Valle. Universidade H4CK3R. 6. ed. São Paulo: Digerati Books, 2009.

[10] M. Sêmola. Gestão da segurança da informação: uma visão executiva. Rio de Janeiro: Campus, 2003.

[11] D. Farmer and W. Venema. Perícia Forense Computacional Teoria e Prática Aplicada. São Paulo: Pearson Prentice Hall, 2006.

COSO - Committee of Sponsoring Organizations of the Treadway Commission. InternalControl – Integrated Framework. New Jersey: COSO, 2008.

FBI, Handbook of Forensics. Disponível online em http://www.fbi.gov/hq/lab/org/cart.htm

ISACA, Cobit 4.1 , Disponível online em isaca.org

ITGI. Information Tecnology Governance Institute. Disponível no site itgi.org

SWGDE, Best Practices for Computer Forensics. Disponível online em http://www.swgde.org/documents/swgde2006/Best_Practices_for_Computer_Forensics%2

Luciana Cantarelli CISA, MBA Gestão de TI, l_cantarelli@hotmail.com, Recife - Brasil

Ananias Queiroga ananiasqueiroga@hotmail.com, Recife - Brasil