Modelagem de ameaças antiforenses aplicada ao processo forense digital

Marcelo B. Maués[1], Bruno Werneck P. Hoelz[2*]

[1]Departamento de Engenharia Elétrica - Universidade de Brasília
[2]Instituto Nacional de Criminalística – Polícia Federal
Brasília, DF – Brasil

marcelomaues76@hotmail.com, werneck.bwph@dpf.gov.br

Abstract: *In digital forensics, the role of the expert is to collect and analyze digital evidence. However, anti-forensics actions threaten the forensic examination process and may compromise its conclusions. This work proposes a threat modeling process in order to reduce the* risks *associated with anti-forensics threats. The proposed process introduces risk management activities as a complement to digital forensic processes found in the literature, allowing a systemic approach for measuring risk and employing countermeasures and risk mitigation strategies.*

Resumo: *Na perícia forense digital, o papel do perito é coletar e analisar as evidências digitais. No entanto, ações antiforenses ameaçam o processo do exame pericial, podendo comprometer suas conclusões. Este trabalho propõe um processo de modelagem de ameaças com o objetivo de reduzir os riscos de ameaças antiforenses. O processo proposto introduz atividades de gestão de risco como um complemento aos processos de perícia digital encontrados na literatura, permitindo uma abordagem sistêmica para a avaliação de risco e o emprego de contramedidas e estratégias de mitigação de risco.*

1 Introdução

A perícia forense digital busca evidências digitais para o esclarecimento de um incidente a partir de informações existentes em diferentes tecnologias, por exemplo, computadores, telefones móveis e redes de computadores (SACHOWSKI, 2016). Esse trabalho é realizado, predominantemente, em ambientes fora do controle do perito, dos quais informações prévias podem ser escassas ou inexistentes. Por isso, a realização do exame pericial requer preparação prévia das ferramentas, técnicas e procedimentos a serem aplicados em cada cenário de atuação.

Um dos aspectos comumente ignorados nessa preparação, é a avaliação de riscos associados a ameaças antiforenses. Essas ameaças estão relacionadas a qualquer tentativa de comprometer a disponibilidade ou utilidade de evidências digitais. Segundo Conlan et al. (2016), meios antiforenses têm se tornado um grande obstáculo para a comunidade forense, exigindo novas iniciativas e estratégias de investigação para resolver esse problema crescente. O resultado antiforense pode ser obtido com o uso de ferramentas ou

* Os autores agradecem o apoio da Secretaria Nacional de Segurança Pública (SENASP), da Diretoria Técnico-Científica da Polícia Federal e da FINEP (Convênio 01.12.0433.01, Projeto: Defesa Nacional e Segurança Pública) na realização deste trabalho.

métodos maliciosos, muitas de conhecimento público, ou simplesmente pelo uso de proteções legítimas como senhas e criptografia.

Apesar da constatação de que ações antiforenses representam uma ameaça ao processo forense digital, tal preocupação não se reflete nos modelos de processos encontrados na literatura, que não consideram a gerência de riscos como uma fase do processo pericial, conforme pode ser observado em Sachowski (2016). Embora diversos estudos sejam realizados sobre detecção de ações antiforenses, como o uso de esteganografia, a ausência de um processo bem definido de identificação e avaliação de riscos contribui para que técnicas de detecção não sejam incorporadas ao processo pericial ou que sejam aplicadas desnecessariamente. No primeiro caso, evidências digitais cruciais ao exame podem deixar de ser recuperadas por falta de tratamento adequado, enquanto no segundo há desperdício de recursos, especialmente de tempo.

Diante dessa realidade, este trabalho propõe um processo de modelagem de ameaças antiforenses para complementar processos propostos na literatura que não consideram tais riscos. O processo proposto também permite que uma organização avalie continuamente seu nível de preparação, seja em termos de treinamento ou das ferramentas disponíveis, identificando lacunas que apresentem risco à realização adequada do exame pericial. Por fim, o processo proposto também auxilia na adoção do preceito de prontidão forense (ou *forensic readiness),* segundo o qual deve-se maximizar o uso de evidências digitais e ao mesmo tempo minimizar custo de uma investigação forense digital (SULE, 2014).

O restante deste artigo está organizado da seguinte maneira: na Seção 2, é discutida a modelagem de ameaças antiforenses aplicada ao processo forense digital; na Seção 3 é demonstrada a aplicação do processo de modelagem proposto através de um estudo de caso e, por fim, na Seção 4, são apresentadas as conclusões e possibilidades de estudos futuros.

2 Modelagem de ameaças antiforenses aplicada ao processo pericial

A modelagem de ameaças é amplamente utilizada no desenvolvimento de software com o objetivo de analisar a segurança do aplicativo, identificando, quantificando e tratando riscos associados ao sistema de uma forma estruturada (OWASP, 2015). Na literatura, é possível encontrar diversas formas de conduzir um processo de modelagem de ameaças, conforme pode ser visto em Sindre e Opdahl (2005), Shostack (2014) e OWASP (2015). Entretanto, no âmbito da perícia digital, os processos propostos na literatura não consideram a gestão dos riscos associados às ameaças antiforenses. Por isso, não foram encontradas aplicações anteriores de técnicas de modelagem de ameaças no processo pericial.

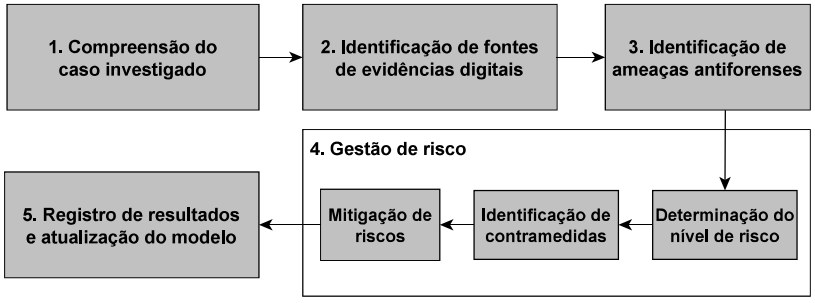

Figura 1 - Processo de modelagem de ameaças antiforenses

O processo de modelagem proposto neste trabalho foi desenvolvido tendo como referência os processos utilizados no desenvolvimento de software. Assim, o modelo de ameaças resultante visa identificar e tratar riscos de ameaças antiforenses que podem afetar a coleta de evidências digitais durante cada uma das fases do processo pericial. O modelo proposto é dividido em cinco etapas, detalhadas a seguir, conforme a Figura 1.

A primeira etapa é de compreensão do caso investigado, cujo objetivo é levantar informações para auxiliar a tomada de decisões em etapas futuras do processo de modelagem. Com base no conhecimento de especialistas, um questionário foi elaborado para nortear a coleta de informações. O questionário está voltado a aspectos relacionados ao suspeito, ao ambiente a ser periciado e a ação criminal, como, por exemplo: há suspeitos com conhecimento avançado de Informática? Que tipos de equipamentos estão envolvidos no incidente?

A identificação das fontes de evidências digitais é a segunda etapa. Nela, são identificados os meios de armazenamento de dados onde podem ser encontradas evidências digitais relacionadas ao incidente. As evidências digitais podem ser obtidas de diversas fontes tais como arquivos produzidos por usuários, *logs* do sistema operacional, históricos de navegadores da Internet ou atributos de arquivos. Também são consideradas fontes de evidências digitais, dispositivos como câmeras digitais, consoles de jogos ou GPS.

Em seguida, é realizada a identificação de ameaças antiforenses**.** Essa etapa consiste em analisar cada uma das fontes de evidências digitais e verificar quais ações antiforenses podem ser aplicadas para comprometê-las. Para auxiliar esta etapa, é proposto um catálogo com registros de ações antiforenses identificadas durante a pesquisa. Por exemplo, criptografia de disco, esteganografia, ocultação de dados em *slack space*[1], entre outros. Seguindo a ideia de busca de ameaças por categorias adotado no modelo STRIDE (SHOSTACK, 2014), amplamente utilizado no desenvolvimento de software, o catálogo é organizado em categorias. As categorias foram definidas com base na classificação de ações antiforenses sugerida por Harris (2006). Segundo o autor, ações antiforenses podem ser classificadas quanto à destruição, ocultação, falsificação e eliminação de fontes das evidências digitais. Cabe ressaltar que o catálogo precisa ser alimentado sempre que se tenha conhecimento de novas técnicas antiforenses.

A gestão de risco é realizada em seguida. Essa etapa tem como objetivo estimar os riscos que as ameaças antiforenses representam ao processo forense digital. Isso permitirá determinar quais delas devem ou não ser mitigadas, pois tratar todas nem sempre é viável tendo em vista os recursos, incluindo o tempo, disponíveis. Essa etapa é discutida em detalhes na seção 2.1.

Por fim, é realizado o registro dos resultados e a atualização do modelo. Nessa etapa, é gerado um relatório com o resultado das etapas anteriores. Assim, é possível recorrer posteriormente a essa documentação para revisar a avaliação realizada pelo perito ou verificar ameaças que porventura não foram consideradas, mas que foram detectadas durante o exame. Essa etapa também é utilizada para a atualização dos catálogos propostos anteriormente: ocorrências de ações antiforenses, ameaças e contramedidas.

[1] Sobras de espaços no disco rígido que não podem ser utilizadas pelo sistema de arquivos

2.1 Gestão de riscos

A gestão de riscos é a principal etapa do processo de modelagem proposto. Ela está divida em três partes: (1) determinação do nível de risco, (2) identificação de contramedidas e (3) mitigação de riscos. A Figura 2 apresenta os elementos envolvidos na gestão do risco. Os três elementos principais são o suspeito, a ameaça e o risco. A motivação, capacidade e oportunidade do suspeito são elementos determinantes na probabilidade da ameaça, enquanto o tipo da ameaça determina seu impacto. A probabilidade e o impacto são então utilizados para determinar o risco.

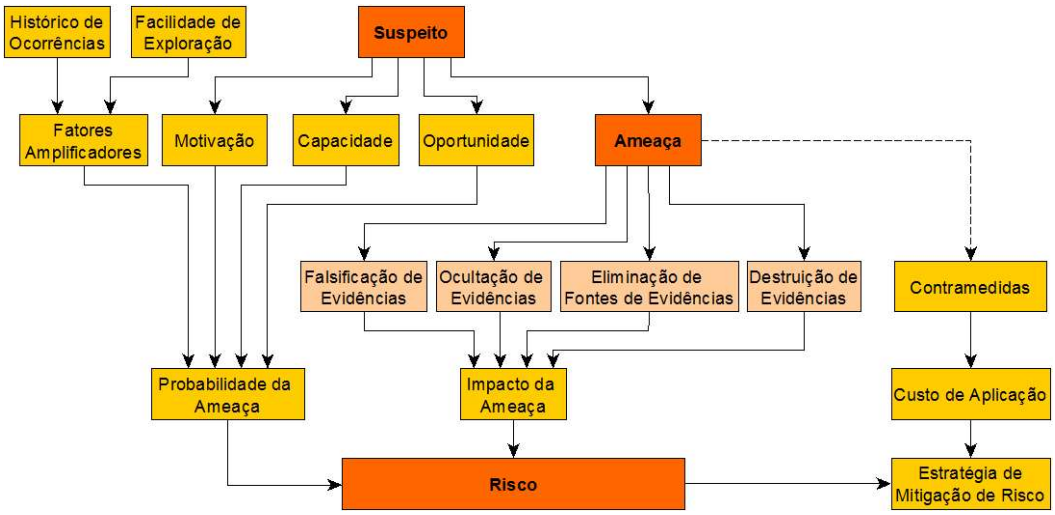

Figura 2 - Elementos envolvidos na gestão de riscos

2.1.1 Determinação do nível de risco

A metodologia proposta para determinação do risco tem como base a publicação especial 800-30 do NIST (*National Institute of Standards and Technology*), bem como as orientações da NBR ISO/IEC 31010:2012, sobre técnicas de avaliação de risco. O nível de risco é determinado pela combinação de fatores relacionados à probabilidade e impacto (NIST, 2002). Neste trabalho, a probabilidade está relacionada à possibilidade de ocorrência da ameaça antiforense e o impacto às consequências que a ameaça antiforense pode causar ao processo forense digital e seus resultados.

Para estimar a probabilidade, são considerados fatores relacionados ao agente da ameaça (suspeito) como motivação, capacidade e oportunidade, fatores considerados determinantes por Vidalis e Jones (2005). A capacidade está relacionada às condições que o suspeito possui para aplicação da ação antiforense. O suspeito tem conhecimento técnico para aplicar a ação antiforense ou conta com profissionais capacitados? Possui condições financeiras para compra de *software* e *hardware*, caso seja necessário? A motivação está relacionada ao custo/benefício do uso de ações antiforenses pelo suspeito. A aplicação de algumas técnicas antiforenses pode ser ou não compensadora para certas ações criminais. Já a oportunidade refere-se às circunstâncias que favorecerem a aplicação da ação antiforense pelo suspeito, como, por exemplo, a existência de uma técnica antiforense pouco documentada e divulgada, inexistência de *software* adequado para tratamento, dificuldade de detecção, etc. Para determinar os fatores de capacidade, motivação e oportunidade relacionados ao suspeito no cálculo da probabilidade da ameaça, são propostas as pontuações apresentadas na Tabela 1.

Além da capacidade, motivação e oportunidade, alguns fatores podem aumentar a probabilidade de ocorrência de uma ação antiforense. Esses fatores são chamados de fatores amplificadores. Segundo Jones (2002), fatores amplificadores são influências que podem contribuir na ocorrência de um incidente. Para o modelo proposto, são fatores amplificadores:

- histórico de ocorrências: relacionado ao emprego anterior da ação antiforense;
- facilidade de exploração: nível de recursos necessário para exploração da ação antiforense. A existência de ferramentas para execução da ação e de documentação do método são exemplos de facilitadores.

Tabela 1 - Pontuação associada à avaliação da capacidade, motivação e oportunidade

Pts.	Capacidade	Motivação	Oportunidade
20	O suspeito possui amplas condições de fazer uso da ação antiforense.	O uso da ação antiforense pelo suspeito compensa muito à prática do delito investigado.	As circunstâncias são altamente favoráveis para aplicação da técnica antiforense.
10	O suspeito possui moderadas condições de fazer uso da ação antiforense.	O uso da ação antiforense pelo suspeito compensa moderadamente à prática do delito investigado.	As circunstâncias são moderadamente favoráveis para aplicação da técnica antiforense.
5	O suspeito possui poucas condições de fazer uso da ação antiforense.	O uso da ação antiforense pelo suspeito compensa pouco à prática do delito investigado.	As circunstâncias são pouco favoráveis para aplicação da técnica antiforense.
0	O suspeito não apresenta condições de fazer uso da ação antiforense.	O uso da ação antiforense pelo suspeito não compensa à prática do delito investigado.	As circunstâncias não são favoráveis para aplicação da técnica antiforense.

Em relação ao "Histórico de Ocorrências", um modelo de catálogo é proposto para registrar ações antiforenses identificadas em exames anteriores ou conhecidas a partir de outras fontes de informação como outros órgãos periciais ou trabalhos científicos. Este catálogo é denominado de catálogo de "Ocorrências de Ações Antiforenses". Para sua eficácia, o catálogo precisa ser atualizado constantemente. Ferramentas e procedimentos utilizados na detecção e tratamento dessas ações são registrados em outro catálogo, de contramedidas, apresentado na Seção 2.1.2.

A Tabela 2 deve ser usada para determinar a pontuação dos fatores amplificadores. A pontuação para cada um dos fatores foi estabelecida de forma que fatores relacionados ao suspeito (capacidade, motivação e oportunidade) fossem suficientes para indicar uma alta probabilidade de ocorrência de uma ação antiforense.

Tabela 2 – Pontuação associada ao histórico de ocorrências e facilidade de exploração

Pts.	Histórico de ocorrências	Facilidade de exploração
20	A ação antiforense foi amplamente utilizada em situações anteriores.	Há diversos facilitadores para aplicação da técnica antiforense.
15	A ação antiforense foi moderadamente utilizada.	Há alguns facilitadores para aplicação da técnica antiforense.
10	A ação antiforense foi pouco utilizada.	Há poucos facilitadores para aplicação da técnica antiforense
0	Não há relatos da aplicação da ação antiforense.	Não há facilitadores para aplicação da técnica antiforense.

Para os fatores amplificadores, a pontuação utilizada visa potencializar a probabilidade de ocorrência, sendo incapaz de, isoladamente, estabelecer uma probabilidade alta de ameaça. No entanto, em ações que são fácil e frequentemente empregadas, a pontuação dos fatores amplificadores aumentaria a probabilidade de ameaça de baixa para média, baixa para alta e de média para alta.

Logo, a probabilidade de ocorrência da ameaça antiforense é estimada pela somatória dos pontos atribuídos a cada um dos fatores e poderá ser baixa (< 45), média (entre 45 e 70) e alta (> 70). Após a determinação da probabilidade de ocorrência da ameaça, é necessário determinar o impacto da ameaça antiforense aos procedimentos pericias. Segundo Beer, Stander e Belle (2014), as ações antiforenses impactam na recuperação e apresentação de evidências com valor probatório, podendo até levar a absolvição de um suspeito. Com base nessa afirmativa, são propostos três níveis de impacto: alto, médio e baixo, conforme a Tabela 3.

Tabela 3 - Níveis de impacto da ameaça

Impacto	
Alto	Pode comprometer totalmente a recuperação e apresentação de evidências digitais utilizáveis.
Médio	Pode comprometer parcialmente a recuperação e apresentação de evidências digitais utilizáveis.
Baixo	Pouco pode comprometer a recuperação e apresentação de evidências digitais utilizáveis.

Por fim, o risco da ameaça antiforense é obtido com a multiplicação da probabilidade pelo impacto, conforme apresentado na Tabela 4. O risco resultante poderá ser alto (entre 50 e 100), médio (de 10 a 50) e baixo (1 a 10).

Tabela 4 - Matriz de cálculo do risco da ameaça antiforense, adaptada de NIST (2002)

Risco = Probabilidade x Impacto			
Probabilidade	**Impacto**		
	BAIXO (10)	MÉDIO (50)	ALTO (100)
ALTO (1,0)	Baixo (1,0 x 10 = 10)	Médio (1,0 x 50 = 50)	Alto (1,0 x 100 = 100)
MÉDIA (0,5)	Baixo (0,5 x 10 = 5)	Médio (0,5 x 50 = 25)	Médio (0,5 x 100 = 50)
BAIXA (0,1)	Baixo (0,1 x 10 = 1)	Baixo (0,1 x 50 = 5)	Baixo (0,1 x 100 = 10)

2.1.2 Identificação de contramedidas

Após a determinação do nível de risco das ameaças, verifica-se a existência de medidas que podem minimizar os impactos nos exames periciais. É proposta a utilização de um catálogo de "Contramedidas", que mantém os procedimentos e ferramentas a serem utilizados para cada situação, bem como observações sobre o custo associado à sua aplicação. O catálogo deve ser atualizado com a descoberta de novas contramedidas.

2.1.3 Mitigação de riscos

Feito o levantamento de contramedidas que podem ser adotadas para minimizar riscos, esta etapa visa avaliar a aplicação ou não delas. A decisão mais adequada está

relacionada ao risco da ameaça e ao custo de aplicação da contramedida. O custo de aplicação pode ser alto, médio e baixo, segundo o esforço necessário para sua aplicação. Algumas medidas podem ser muito custosas e, dependendo do risco da ameaça, podem ser julgadas desnecessárias. Cabe ressaltar que a determinação do custo de aplicação da contramedida depende dos recursos, inclusive tempo, disponíveis para o perito ou órgão pericial.

Para auxiliar a decisão de aceitar ou não o risco da ameaça, uma matriz composta por valores do risco da ameaça e custo de aplicação da contramedida é proposta (Tabela 5). A combinação do risco e custo na matriz resulta em dois valores: mitigar ou aceitar. O primeiro valor (mitigar) significa que a aplicação da contramedida é indicada diante do risco da ameaça, ou seja, a contramedida deve ser aplicada. Já o segundo valor (aceitar) significa que o risco da ameaça deve ser aceito, já que o custo não compensa em face do risco avaliado. Como os custos de aplicação dependem dos recursos disponíveis, a estratégia de mitigação pode variar de uma aplicação para outra, em especial se vários riscos forem identificados. Algumas ameaças de baixo risco podem ser toleradas em face a uma ameaça simultânea de médio risco, caso os recursos para tratá-las sejam limitados. Portanto, o nível de risco não determina, isoladamente, a obrigatoriedade de qualquer ação por parte do perito. É necessário também avaliar o custo de mitigação desses riscos.

Tabela 5 - Matriz de estratégia de mitigação

Estratégia de Mitigação			
Risco	**Custo de aplicação**		
	BAIXO	MÉDIO	ALTO
ALTO	Mitigar	Mitigar	Mitigar
MÉDIO	Mitigar	Mitigar	Aceitar
BAIXO	Mitigar	Aceitar	Aceitar

3 Estudo de caso

Para validar o processo proposto, considerou-se um caso real de busca e apreensão realizado em uma empresa privada. A investigação apurava crime de exploração e abuso sexual de criança ou adolescente. Nos próximos parágrafos, são apresentados resumidamente os resultados obtidos em cada etapa da aplicação do processo de modelagem de ameaças antiforenses conduzidos pelo Perito designado para participar da operação.

Na primeira etapa (compreensão do caso investigado), com o suporte do questionário proposto, apurou-se que o caso envolvia um funcionário, lotado na Gerência de Informática, com conhecimentos avançados de informática, sem antecedentes criminais e com idade aproximada de 30 anos. Em termos de equipamentos computacionais, a operação previa apenas a apreensão do computador de uso diário do funcionário.

Na segunda etapa (identificação de fontes de evidências digitais), foram considerados como fontes potenciais de evidências digitais apenas arquivos de imagem e vídeo produzidos pelo usuário armazenados no disco rígido do computador.

Na terceira etapa (identificação de ameaças antiforenses), com suporte do catálogo de ameaças antiforenses, foram identificados diversos tipos de ameaças antiforenses que poderiam comprometer a recuperação de arquivos de imagem e vídeo. Contudo, neste trabalho, serão consideradas apenas as ameaças de ocultação de dados com uso de criptografia de disco (*full-disk encryption*) ou esteganografia.

Na quarta etapa (gestão de riscos), primeiramente foram estimados a probabilidade e o impacto e, em seguida, foi estimado o risco efetivo da ameaça utilizando a matriz de risco proposta no modelo. A Tabela 6 apresenta os resultados obtidos.

Tabela 6 - Estudo de caso: cálculo da probabilidade, impacto e risco

Ameaça antiforense	Probabilidade	Impacto	Risco (Probabilidade x Impacto)
Criptografia de disco	Capacidade + Motivação + Oportunidade + Histórico de Ocorrências + Facilidade de Exploração = 20 + 20 + 20 + 15 + 20 = 95 (Alta)	Alto (pode comprometer totalmente a recuperação e apresentação de evidências digitais utilizáveis)	Alta x Alto = Alto
Esteganografia	Capacidade + Motivação + Oportunidade + Histórico de Ocorrências + Facilidade de Exploração = 20 + 20 + 20 + 0 + 10 = 70 (Média)	Médio (pode comprometer parcialmente a recuperação e apresentação de evidências digitais utilizáveis)	Média x Médio = Médio

Estimado o risco, contramedidas foram sugeridas para cada ameaça, com apoio do catálogo de contramedidas. Cabe ressaltar que na inexistência de soluções no catálogo, outras fontes devem ser pesquisadas. Em seguida, foi feito uma análise do custo de aplicação das contramedidas para cada ameaça. A Tabela 7 apresenta as contramedidas propostas, seu custo e algumas observações sobre sua aplicação.

Tabela 7 - Estudo de caso: contramedidas identificadas e custo de aplicação

Ameaça antiforense	Contramedidas	Custo	Observações
Criptografia em disco	Obtenção dos volumes criptografados quando ainda estão montados (CM1).	Médio	Requer oportunidade adequada para realização da cópia dos dados (cujo tempo depende do volume de dados encontrado).
	Obtenção da chave criptográfica do volume (CM2).	Alto	Não há garantia de sucesso, mesmo com grande custo de tempo.
Esteganografia	Busca por ferramentas ou aplicações de esteganografia no computador do suspeito. Se forem encontradas, indagar o suspeito sobre sua utilização (CM3).	Baixo	A verificação de ferramentas conhecidas pode ser feita facilmente (caso não haja outro obstáculo), mas não é exaustiva.
	Analisar o conteúdo de arquivos com ferramentas de detecção automatizada, como s*tegdetect* (CM4).	Alto	O tempo de execução das ferramentas pode ser proibitivo dependendo do volume de dados.

Com a combinação do custo de aplicação e risco da ameaça na matriz de estratégia de mitigação sugerida no modelo, é definido se o risco da ameaça deve ser aceito ou se as contramedidas devem ser aplicadas (mitigar). A Tabela 8 apresenta esses resultados e

mostra que nem todas as contramedidas devem ser aplicadas. Por exemplo, para ameaça esteganografia foram sugeridas 02 (duas) contramedidas: CM3 e CM4. Contudo, a contramedida CM4 não deverá ser aplicada, visto que, seu custo de aplicação alto não compensa diante do risco médio da ameaça esteganografia.

Tabela 8 – Estudo de caso: estratégia de mitigação

Risco da ameaça antiforense	Custo de aplicação da contramedida	Estratégia de mitigação
Criptografia em disco: Alto	CM1: Médio	Mitigar
	CM2: Alto	Mitigar
Esteganografia: Médio	CM3: Baixo	Mitigar
	CM4: Alto	Aceitar

Na última etapa, um relatório foi gerado com todos os resultados da aplicação do processo de modelagem de ameaças antiforenses, bem como da constatação de fato dessas ameaças e do emprego das contramedidas. No caso em questão, não foram identificadas ameaças de esteganografia com o uso da busca por ferramentas ou aplicações conhecidas para esse fim. A ameaça de criptografia de disco também não foi confirmada, embora a contramedida CM1 tenha sido aplicada preventivamente, considerando que a confirmação da ameaça só seria possível após o acesso ao computador.

4 Conclusões

Este trabalho propôs a aplicação do processo de modelagem de ameaças no tratamento de riscos de ações antiforenses em processos forenses digitais. O modelo, dividido em cinco etapas (compreensão do caso investigado, identificação de fontes de evidências, identificação de ameaças, gestão de riscos e registro dos resultados), complementa as fases comumente utilizadas no processo forense digital, introduzindo a gestão de risco de ações antiforenses que possam prejudicar o resultado da atividade pericial. A proposta também contribui para complementar o processo pericial ao sugerir a adoção de um questionário para auxiliar o levantamento de informações sobre o caso investigado e de catálogos que servem de fontes de informações para auxiliar na tomada de decisões durante a aplicação do modelo de ameaça.

O estudo de caso demonstra que a incorporação do modelo proposto nas atividades do perito permite identificar e avaliar riscos de ameaças antiforenses ainda no início do processo e oferecer medidas de detecção e mitigação que podem ser aplicadas nas fases de coleta e análise de dados. Com isso, o processo pericial torna-se mais robusto, minimizando perdas de evidências digitais diante de riscos antiforenses.

Em nível organizacional, a utilização do processo proposto, incluindo a atualização constantes dos catálogos propostos, permite avaliar o nível de preparação para atender determinadas ameaças. Pode-se, por exemplo, identificar a indisponibilidade de ferramentas para detecção de esteganografia ou a necessidade de abordar um suspeito enquanto um volume criptografado está disponível no computador. Alguns riscos que podem parecer improváveis para determinadas organizações podem se apresentar críticos em outros (uso de esteganografia em casos associados a terrorismo). Portanto, a forma de aplicação da proposta depende da realidade objetiva encontrada pelos peritos. Cabe destacar que a gestão de risco no processo forense também é preventiva, em preparação às ameaças antiforenses, e não somente reativa. Portanto, algumas contramedidas

implicam em ações de planejamento anteriores à realização da coleta de dados e exame pericial, como foi possível observar no estudo de caso.

Trabalhos futuros devem ser realizados na expansão dos catálogos de ameaças e contramedidas, bem como em formas de compartilhamento desse conhecimento entre organizações. Naturalmente, a aplicação do processo proposto torna-se mais eficiente com uma base de conhecimento mais abrangente e com um histórico de ocorrências que permite ao perito avaliar com maior precisão os riscos envolvidos em determinado cenário.

Referências bibliográficas

BEER, R., STANDER, A. & BELLE, J. V. (2014). Anti-Forensic Tool Use and Their Impact on Digital Forensic Investigations : A South African Perspective. Department of Information Systems. University of Cape Town Private. Conference Paper.

CONLAN, K., BAGGILI, I. e BREITINGER, F. (2016). Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy. Digital Investigation, 18(December 2015), S66–S75

HARRIS, R. (2006). Arriving at an Anti-Forensics Consensus: Examining How to Define and Control the AntiForensics Problem. Digital Investigation, 3(S), S44-S49. Disponível em http://dfrws.org/2006/proceedings/6-Harris.pdf.

ISO/IEC 31010. (2012). ABNT NBR ISO/IEC 31010:2012. Gestão de riscos — Técnicas para o processo de avaliação de riscos. ABNT - Associação Brasileira de Normas Técnicas. 04/04/2012.

JONES, A. (2002). Identification of a Method for the Calculation of Threat in na Information Environment, 44(abril).

NIST. (2002). Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology (NIST). Special Publication 800-53. Department of Commerce.

OWASP.(2015). Application Threat Modeling. Open Web Application Security Project. Disponível em https://www.owasp.org/index.php/Application_Threat_Modeling.

SACHOWSKI, J. (2016). Implementing Digital Forensic Readiness: From Reactive to Proactive Process. Syngress.

SHOSTACK, A. (2014). Threat Modeling: Designing for Security. John Wiley & Sons, Inc., Indianapolis, Indiana.

SINDRE, G. e OPDAHL, A. L. (2005). Requirements Eng. Eliciting security requirements with misuse cases. Disponível em https://link.springer.com/article/10.1007/s00766-004-0194-4

SULE, D. (2014). Importance of Forensic Readiness. ISACA Journal. Disponível em http://www.isaca.org/Journal/archives/2014/Volume-1/Pages/JOnline-Importance-of-Forensic-Readiness.aspx.

VIDALIS, S. e JONES, A. (2005). Analyzing Threat Agents and Their Attributes. Disponível em https://www.researchgate.net/publication/220947230_Analyzing_Threat_Agents_and_Their_Attributes.

