UNIVERSIDADE DO SUL DE SANTA CATARINA

THEODORO AREEL MATTOSO NETO

FORENSE COMPUTACIONAL:
UM ESTUDO DE APLICAÇÕES DE MÉTODOS INVESTIGATIVOS FORENSE EM AMBIENTES CORPORATIVOS

Palhoça

2014

THEODORO AREEL MATTOSO NETO

FORENSE COMPUTACIONAL:
UM ESTUDO DE APLICAÇÕES DE MÉTODOS INVESTIGATIVOS FORENSE EM AMBIENTES CORPORATIVOS

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Ciência da Computação da Universidade do Sul de Santa Catarina, como requisito parcial à obtenção do título de Bacharel em Ciência da Computação.

Orientador: Prof. Luiz Otavio Botelho Lento.

Palhoça

2014

THEODORO AREEL MATTOSO NETO

FORENSE COMPUTACIONAL:
UM ESTUDO DE APLICAÇÕES DE MÉTODOS INVESTIGATIVOS FORENSE EM AMBIENTES CORPORATIVOS

Este Trabalho de Conclusão de Curso foi julgado adequado à obtenção do título de Bacharel em Ciência da Computação e aprovado em sua forma final pelo Curso de Graduação em Ciência da Computação da Universidade do Sul de Santa Catarina.

Palhoça, 11 de Junho de 2014.

_____

Professor e orientador Luiz Otávio Botelho Lento, Me.
Universidade do Sul de Santa Catarina - UNISUL

_____

Prof. Flávio Ceci, Me.
Universidade do Sul de Santa Catarina - UNISUL

_____

Prof. Théo Augustus Luz, Esp.
Universidade do Sul de Santa Catarina - UNISUL

A minha família, que sempre me apoiou em todos os momentos de minha vida, e principalmente no fim de minha formação e na elaboração deste trabalho.

AGRADECIMENTOS

A Altair Areel Mattoso, Debora Gomes de Araújo Mattoso, Irene Ilda Gomes de Araújo, Sônia Cardoso Antonietti, Regina Helena Antonietti Mattoso, Daisy Gomes de Araújo, Marco Antônio Gomes de Araújo, Paulo Rogério Tavares da Silva, Andrea Mattoso Sauda, Victor Mattoso Sauda, Carolina Mattoso Sauda, Fernanda Mattoso Silva, Viviane de Souza, Vanice Maria Jacoboski, Denis Diniz, Luiz Ricardo Guarezzi, Mateus Lohn Andriani, Max Diogo Vieira, Felipe Mayer Pereira, Karine Koller, Aran Bey Tcholakian Morales, Sandra Regina Martins, Heloise Ruschel, Flávio Ceci, Theo Luz, e por fim, agradeço a Luiz Otavio Botelho Lento, que me despertou o interesse no segmento de mercado da segurança da informação, e me inspirou a almejar a carreira de perito forense da polícia federal do Brasil.

“Uma jornada de mil quilômetros começa com um passo. ” (Lao Tzu, 551 a.C).

RESUMO

Forense se dá pelo conjunto de técnicas investigativas aplicadas de modo a se resolver ou desvendar um crime partindo de dados dispersos no meio em que o suposto crime ocorreu, e organizando-os de modo a se produzir evidências.

Evidências que tratadas com a aplicação de leis podem vir a se tornar provas, sendo utilizadas diretamente em tribunais de casos criminais, ou trabalhistas.

Neste trabalho o foco se encontra na aplicação de tais técnicas dentro de um ambiente de rede corporativo, sendo este o ambiente aplicável mais relevante tendo em vista o tamanho do fluxo de dados, valor das informações por ali trafegadas, e confidencialidade das mesmas.

Para isso o perito deve dispor de conhecimentos de segurança da informação, redes, e sistemas operacionais, de modo que concentre capacitação técnica o suficiente para realizar uma investigação completa e produzir um laudo pericial ao final do ciclo investigativo.

Com isso em mente este trabalho possui um embasamento teórico focado em revisões bibliográficas do ramo de segurança da informação como base do estudo, apresentando conceitos chave como criptografia, controle de acesso, planos de ação, gestão de segurança da informação, normas técnicas de aplicação de uma política de segurança, e aí sim, apresenta os tipos de forense computacional, no que consiste tal expressão e ramo da segurança, quais os tipos de estratégias adotadas ao se planejar uma investigação, e, por fim, o autor elabora um modelo conceitual e sequencial de investigação forense embasado por todos estes conceitos, de modo a exemplificar, viabilizar e contextualizar o quão importante é este tipo de investigação e quais as vantagens que decorrem da aplicação correta deste modelo em cenário corporativo.

Palavras-chave: Segurança. Informação. Forense. Estática. Dinâmica. *Firewall*. Rede. Computação. Linux. Controle. Acesso. Dados. Criptografia. Cifra. *Backup*. SGSI. PDCA. Planejamento. Análise. Coleta. Evidência. Prova. Isolamento. Tratamento. Identificação. Autenticação.

ABSTRACT

Forensics can be defined by de gathering of investigatives techniques applied with the intent of solving crimes from scaterred data in the crime scene, organising such data for the assembly of evidences.

These evidences must be legally treated, so that it can be turned into proof that can be used in civilian or working cases on court.

This paper focuses on the application of such techniques in a corporate network, the relevance of a corporate network lies on the data flow and information value that runs throught, not to mention the number of classified informations that need protection.

To be able to accomplish that goal, the forensic expert must have extensive knowledge of information security, networks and operating systems, so that he or she can have the right amount of expertise to effectively perform a forensic investigation, and produce undisputed proof of what actually happened.

With that in mind this paper gathered literal background focusing on information security with a focus point on several themes like, cryptography, access control, action plans, information security administration, technical rules of engagement for a information security policy, and only then, present the concepts of digital forensics, such as dead forensics (static forensics) and live forensics (dynamic forensics, and establishes a sequential forensic investigation concept mode based on all information security background gathered throughout the makings of this paper, and to what ends such model can be useful, valid, and advantageous to a corporation.

Keywords: *Security*. *Information*. *Forensics*. *Static*. *Dynamic*. *Firewall*. *Network*. *Computing*. Linux. *Control*. *Access*. *Data*. *Cryptography*. *Cypher*. *Backup*. SGSI. PDCA. *Planning*. *Analysis*. *Gathering*. *Evidence*. *Proof*. *Isolation*. *Treatment*. *Identification*. *Authentication*.

LISTA DE QUADROS

Quadro 1 – Método de análises de risco 57

LISTA DE TABELAS

Tabela 1 - Grau de ameaça quanto a análise de riscos 58
Tabela 2 - Grau de vulnerabilidade quanto a análise de riscos 58
Tabela 3 - Grau de impacto quanto a análise de riscos 59
Tabela 4 - Cronograma simplificado 70
Tabela 5 - Cronograma detalhado - Março 2014 70
Tabela 6 - Cronograma detalhado - Abril 2014 71
Tabela 7 - Cronograma detalhado - Maio 2014 71

LISTA DE ILUSTRAÇÕES

Figura 1 - Informação é a base do conhecimento 16
Figura 2 - Esquema de funcionamento de criptossistemas 42
Figura 3 - Processo de um criptossistema híbrido 44
Figura 4 - Componentes dos requisitos de negócio da GeSI 47
Figura 5 - O ciclo PDCA 52
Figura 6 - Ciclo de uma investigação forense 69
Figura 7 - Formulário de cadeia de custódia 76
Figura 8 - Atributos de tempo 77
Figura 9 - Execução do *cryptcat* 79
Figura 10 - *Status* de uso de sistemas operacionais no mundo em 2014 92
Figura 11 - NESSUS em execução 93
Figura 12 - RETINA em execução, exibição de relatórios 95
Figura 13 - *WIRESHARK* em modo de captura 96
Figura 14 - Modelo Conceitual 100
Figura 15 - AES *Symmetric Ciphers Online* 119
Figura 16 - MD5 *HASH GENERATOR* 120

SUMÁRIO

1 INTRODUÇÃO 15
1.1 PROBLEMA 17
1.2 OBJETIVOS 18
1.2.1 Objetivo geral 18
1.2.2 Objetivos específicos 18
1.3 JUSTIFICATIVA 19
1.4 ESTRUTURA DA MONOGRAFIA 20
2 REVISÃO BIBLIOGRÁFICA 22
2.1 INFORMAÇÃO 22
2.1.1 Ativo da Informação 24
2.2 SEGURANÇA DA INFORMAÇÃO 25
2.2.1 Confidencialidade 26
2.2.2 Integridade 26
2.2.2.1 Autenticação 27
2.2.2.2 Não Repúdio 27
2.2.2.3 Legalidade 28
2.2.2.4 Privacidade 28
2.2.2.5 Auditoria 29
2.2.3 Disponibilidade 29
2.2.4 Vulnerabilidade 30
2.2.5 Ameaças 30
2.2.5.1 Ataques 31
2.2.5.2 Tipos de ataque 31
2.2.5.2.1 Ataque físico 32
2.2.5.2.2 Packet sniffing 32
2.2.5.2.3 Port scanning 33
2.2.5.2.4 Scanning de vulnerabilidades 34
2.2.5.2.5 Denial of service 34
2.2.5.2.6 Ataques a nível de aplicação 35
2.2.5.3 Atacantes 36
2.2.5.3.1 Script Kiddies 36
2.2.5.3.2 Crackers 37
2.2.5.3.3 Carders 37
2.2.5.3.4 Cyberpunks 38
2.2.5.3.5 Insiders 38
2.2.5.3.6 Coders 38
2.2.5.3.7 White Hats 39
2.2.5.3.8 Black Hats 39
2.2.5.3.9 Gray Hats 40
2.2.5.3.10 Phreackers 40
2.2.6 Criptografia 40
2.2.6.1 Criptossistemas Simétricos 43
2.2.6.2 Criptossistemas Assimétricos 43
2.2.6.3 Criptossistemas Híbridos 44
2.2.6.4 Importância da Criptografia 45
2.3 GESTÃO DE SEGURANÇA DA INFORMAÇÃO 46
2.3.1 Requisitos de Gestão da Segurança da Informação 47
2.3.1.1 Requisitos Comerciais 48

2.3.1.2 Requisitos Legais 48
2.3.1.3 Gerenciamento das Fronteiras da Informação 49
2.3.1.4 Compartilhando a Informação 50
2.3.1.5 Abordagem Holística 50
2.3.2 Sistema de Gestão de Segurança de Informação (SGSI) 51
2.3.3 O SGSI e o ciclo PDCA (*Plan Do Check Act*) 51
2.3.4 Requisitos de um SGSI de acordo com o estabelecido pela norma NBR ISO/IEC 27001:2005 52
2.3.4.1 *Plan* (Planejamento) 52
2.3.4.2 *Do* (Executar) 54
2.3.4.3 *Check* (Verificar) 55
2.3.4.4 *Act* (Monitoramento) 56
2.3.5 Análise de Riscos 56
2.3.5.1 Estratégia de avaliação de risco 57
2.3.6 Política de Gestão de Segurança da Informação 60
2.3.6.1 Importância de uma política de segurança 60
2.3.7 Implantação do SGSI 61
2.3.7.1 Requisitos para a implantação do SGSI 61
2.3.8 Auditoria 62
2.3.8.1 Auditoria de primeira parte 63
2.3.8.2 Auditoria de segunda parte 63
2.3.8.3 Auditoria de terceira parte 63
2.3.9 Aspectos de uma auditoria 64
2.3.9.1 Pesquisa das fontes de informação 64
2.3.9.1.1 O que/onde coletar 64
2.3.9.2 Campo, âmbito e subáreas 65
2.3.9.3 Recursos necessários 65
2.3.9.4 Metodologias 65

3 MÉTODO 67
3.1 CARACTERIZAÇÃO DO TIPO DE PESQUISA 69
3.2 DELIMITAÇÕES DO PROBLEMA 71

4 ANÁLISE DA APLICAÇÃO DE MÉTODOS FORENSE PARA AMBIENTES CORPORATIVOS. 73
4.1 TIPOS DE FORENSE COMPUTACIONAL 73
4.2 FORENSE ESTÁTICA (*STATIC FORENSIC*) 74
4.2.1 Análise estática 75
4.2.1.1 Cópia lógica (*backup*) 77
4.3 FORENSE DINÂMICA (*LIVE FORENSIC*) 78
4.3.1 Análise de memória volátil 78
4.3.2 *Cryptcat* capturando memória volátil 79
4.4 PREPARAÇÃO 80
4.5 COLETA 81
4.5.1 Dispositivos de armazenamento 82
4.5.2 Alterações no sistema 83
4.6 ANÁLISE 84
4.7 RECONSTRUÇÃO DE EVENTOS 85
4.8 FERRAMENTAS PARA MONITORAMENTO 85
4.8.1 Coletando dados brutos 86
4.8.2 Estado da rede 87
4.8.3 Coletando informações sobre o estado do sistema 88
4.8.4 Informações do sistema de arquivos 88
4.8.5 Informações do alvo 89
4.8.6 Varreduras de sistema 90
4.8.7 Ganhando acesso ao sistema 90

4.8.8 Mantendo o acesso no sistema 91
4.9 FERRAMENTAS PARA ANÁLISE 91
4.9.1 Sistema Operacional - SO 92
4.9.1.1 *Microsoft™ Windows®* 8.1.... 92
4.9.1.1.1 NESSUS 93
4.9.1.1.2 RETINA....94
4.9.1.1.3 WIRESHARK 95
4.9.1.2 Linux Kali 1.0.6 via Oracle™ VirtualBox 97

5 MODELO CONCEITUAL.... 100
5.1 IDENTIFICAÇÃO....100
5.2 PLANEJAMENTO....102
5.3 ISOLAMENTO 103
5.4 COLETA....104
5.5 ANÁLISE 105
5.6 TRATAMENTO....106
5.7 COMPILAÇÃO 106

6 EXECUÇÃO DO MODELO EM ESTUDO DE CASO 108
6.1 IDENTIFICAÇÃO, ENTENDENDO O PROBLEMA 108
6.2 PLANEJAMENTO, DEFININDO UM RUMO....114
6.2.1 Analisando o levantamento de dados sobre o possível incidente 115
6.2.2 Definindo estratégias de investigação....116
6.2.3 Definindo ferramentas....117
6.3 ISOLAMENTO: ISOLANDO A ÁREA DE INVESTIGAÇÃO E APLICAÇÃO DE ESTRATÉGIAS....120
6.4 COLETA: COLETANDO MASSA DE DADOS 122
6.5 ANÁLISE: SEPARANDO AS EVIDÊNCIAS DA MASSA DE DADOS....122
6.6 TRATAMENTO: APLICANDO LEIS ÀS EVIDÊNCIAS ANALISADAS....124
6.7 COMPILAÇÃO: ELABORAÇÃO DE PROVAS....126

7 CONCLUSÃO 128
7.1 TRABALHOS FUTUROS 129
7.2 CONSIDERAÇÕES FINAIS 130

REFERÊNCIAS 132

APÊNDICES.... 135

APÊNDICE A – TRECHO DE TEXTO CIFRADO UTILIZANDO AES – *SYMMETRIC CIPHERS ONLINE* 136

APÊNDICE B – *LOGS* DE *E-MAILS* ENVIADOS PELA EQUIPE DE DESENVOLVIMENTO 137

APÊNDICE C – *E-MAIL* CAPTURADO À EMPRESA CONCORRENTE.... 138

APÊNDICE D – LISTA DE *E-MAILS* ENVIADOS À EMPRESA CONCORRENTE 139

APÊNDICE E – LISTA DE *E-MAILS* ENVIADOS AO COLABORADOR PELA EMPRESA CONCORRENTE 140

1 INTRODUÇÃO

A ciência forense ou criminalística é o processo de usar o conhecimento científico na coleta, análise e apresentação de vestígios para que estas se constituam provas em um processo judicial. (MADEIRA, 2012, p.13).

Segundo o Dicionário *Priberam* da Língua Portuguesa (2011), a palavra “forense” significa “de foro judicial” ou “dos tribunais ou a ele relativos”, com esse conceito, entende-se que todas as práticas forenses, de alguma forma, sempre estão ligadas ao cumprimento da lei, ou à constituição, sendo em suma, uma prática policial e investigativa, independente da área de atuação do perito forense.

Com a popularização da internet em todo o mundo, milhares de pessoas começaram a se utilizar deste meio. Contemporaneamente se percebe que nem todos a utilizam de maneira sensata, e acreditando que a internet é um espaço livre, acabam por exceder em suas condutas e criando novas modalidades de delito: os crimes virtuais. (PINHEIRO, 2000, p.1).

Com o conceito apresentado por Pinheiro (2000), vê-se a necessidade de existir uma maneira de prevenir, e rastrear os crimes virtuais, cria-se então, a computação forense, como ramo ativo da área de segurança de informação.

Lyra (2008) apresenta um argumento de que, segurança da informação é um assunto muito discutido na atualidade, e possui várias vertentes que a definem e a conceituam. Com isso, e com a consciência de que o mundo hoje está *online*, este segmento da segurança de informação torna-se imprescindível para as corporações, bem como para os usuários ditos “comuns”, ou seja, que utilizam do computador apenas para uso pessoal (mas que não deixam de estar em risco.).

Em verdade, a repressão dos cyber crimes também tem encontrado barreiras referentes a conquista de provas materiais. A internet propicia, devido a sua rapidez, a possibilidade de serem eliminados a qualquer momento quaisquer **vestígios** necessários para a comprovação do delito. (PINHEIRO, 2000, p.2).

Uma investigação pode envolver o exame de todos esses tipos de dados, dependendo das circunstâncias. Obter os dados latentes é de longe o que requer mais recurso e tempo. (MADEIRA, 2012, p.16). Vista a dificuldade da obtenção de tais dados, além da complexidade de se analisar os mesmos.

Com tudo, enxerga-se claramente que a computação forense aborda a informação como ponto de partida e de chegada, sendo a chave, e a barreira ao mesmo tempo, dependendo de como ela se apresenta, e de como seria a melhor forma de investiga-la.

O grande problema, como dito por Campos (2007), é que a própria definição da palavra “informação” é ambígua e incerta, variando entre diversas áreas de trabalho, culturas e ciências. Porém, há pelo menos um consenso mínimo onde é falado que a informação é ao mesmo tempo composta de dados e componentes do conhecimento como um todo, onde se é possível observar que dados aparentemente aleatórios em um meio, podem ser quantificados e qualificados de modo a se construir informação, que posteriormente deve ser também quantificada e qualificada de modo a se obter conhecimento.

Esta observação exemplifica a complexidade de se manipular, definir e classificar informação, complexidade esta que influencia diretamente na elaboração deste trabalho como um todo, e influencia também na capacitação técnica necessária para uma investigação forense, e para o ramo de segurança da informação em geral.

Essa complexidade pode ser simplificada em um simples diagrama na figura 1, ilustrando o processo previamente descrito.

Figura 1 - Informação é a base do conhecimento

Fonte: CAMPOS (2007, p.17).

Partindo do explicado, e ilustrado pela figura, entende-se a importância da informação para o mundo, justamente por ser atrelada, e matéria prima para o conhecimento, então, seja qual for o objetivo a informação então precisa ser protegida, e mantida de modo a não sofrer quebra nenhuma de integridade.

Apresentado o conceito introdutório deste trabalho, o primeiro capítulo é dividido em **Problema**, onde apresentam-se as perguntas motivadoras da pesquisa realizada, **Objetivos**, que representam onde o autor deseja chegar, especificamente e em uma visão geral, e finalmente, a **Justificativa** do tema escolhido para este trabalho, procurando esclarecer o motivo por trás do desenvolvimento da proposta aqui presente.

1.1 PROBLEMA

No meio empresarial, ou no ambiente corporativo, como abordado neste trabalho, a informação torna-se o centro das atenções, o bem mais importante da empresa, Campos (2007) comprova esta afirmação dizendo que "a informação é um elemento essencial para a geração do conhecimento, para a tomada de decisões, e que representa efetivamente valor para o negócio, dentro de cada um de seus processos. "

Dito por Carvalho (2005) os crimes virtuais já são realidade, podendo atingir desde pessoas simples que possuem uma conta bancária até grandes empresas que têm informações confidenciais que possuem valor comercial (informações essas, que em caso de se tornarem públicas, podem representar danos materiais enormes para a corporação).

Sendo assim, surge a necessidade de se identificar, mensurar e registrar esses tipos de atividades, que em geral são chamados de incidentes de segurança. (CARVALHO, 2005, p.9).

Como então proteger a informação? Para responder essa pergunta, é interessante abordar no tema mais comum em termos de segurança da informação, a **criptografia**.

A criptografia existe desde que o homem se agrupou em sociedades que eram mais ou menos organizadas (MARTINI, 2001, p.2).

Segundo o nosso *Aurélio* temos ***criptografia quando escrevemos em cifra ou em código*** (MARTINI, 2001, p.3).

Basicamente então, criptografia é uma técnica utilizada para transformar um texto limpo (*plaintext*) em texto cifrado, podendo utilizar diversas técnicas para tal, variando a metodologia, deixando a informação protegida por cifras, evitando que se "monte" um conhecimento a partir do dado obtido por algum ataque.

Porém este é somente um dos métodos que podem ser utilizados para que se proteja a informação em uma corporação, e para que se responda as perguntas de motivação a este trabalho, "Como proteger a informação? Como detectar um incidente de informação? Quais medidas tomar para que o incidente detectado não volte a ocorrer? Como provar que um crime digital foi efetuado? ".

1.2 OBJETIVOS

Os objetivos deste trabalho, são centrados em responder às perguntas levantadas na problemática, de modo a estudar, exemplificar e expôr métodos de investigação forense adequados às situações corporativas gerais (não abordando um porte, ou cenário específicos).

1.2.1 Objetivo geral

Este trabalho tem por objetivo compreender o conceito de forense computacional, bem como seus métodos, variações, e aplicação em ambiente corporativo.

1.2.2 Objetivos específicos

- Compreender os conceitos e princípios de segurança da informação Apresentar e contextualizar as variações da forense computacional
- Entender a aplicação desses métodos
- Analisar as principais ferramentas e ambientes utilizados para possibilitar a execução dos procedimentos previstos pela forense computacional.
- Bolar um modelo de investigação conceitual utilizando o embasamento teórico apresentado
- Montar uma estrutura empírica representando um estudo de caso viável para a aplicação do modelo proposto

Com os objetivos estabelecidos, o propósito do trabalho e a escolha do tema se caracterizam pela justificativa presente a seguir.

1.3 JUSTIFICATIVA

A justificativa deste trabalho encontra-se na atualidade do tema, em razão da importância da informação nos dias de hoje.

Parafraseando Lyra (2008), as preocupações com a segurança das redes devem abranger todos os problemas, desde autenticação de usuário, até equipamentos de restrição dos usuários aos serviços autorizados, contemplando o estabelecimento de interfaces seguras entre as redes internas e externas, sendo públicas, ou de outras organizações.

Campos (2007) estabelece que há uma consideração a ser feita sobre essas informações: as informações que sustentam os processos da organização estão informatizadas? Se a resposta for sim, o SGSI (*Sistema de Gestão de Segurança de Informação*) deve ser implantado primeiramente na área de Tecnologia da Informação, pois isso garantiria minimamente a confidencialidade, a integridade e a disponibilidade das informações.

A citação acima mostra que, apesar de ser um conceito comum, que o mundo de hoje está *online*, é sempre possível, e prudente, ponderar que, talvez nem tudo esteja em rede. Sempre se deve considerar que alguma massa de informação pode estar *off-line* armazenada em meio físico.

Analisando os *reports* de invasões, e espionagem de dados importantes, como o incidente de espionagem americana à presidente do Brasil Dilma Rousseff em Agosto de 2013, pode-se chegar à conclusão que por mais moderna que seja a tecnologia presente em servidores, e na rede em si, o assunto ainda é problema, e ainda precisa ser estudado cuidadosamente, para que cada vez mais se aperfeiçoe as técnicas de segurança da informação e investigação de incidentes de segurança, de modo que se prove um crime, ou tentativa de um crime, e se possam tomar medidas preventivas de novos tipos similares de incidentes.

1.4 ESTRUTURA DA MONOGRAFIA

Esta monografia se encontra definida por 7 (sete) capítulos descritos a seguir.

- **Capítulo 1 - Introdução**: Aqui é definido o tema, o problema, os objetivos, a justificativa, e é apresentada uma introdução do assunto geral abordado pelo restante do trabalho.

- **Capítulo 2 – Revisão bibliográfica**: Este capítulo foca nos conceitos gerais de segurança da informação como criptografia, atacantes, incidentes de informação, ataques e gestão de segurança da informação.

- **Capítulo 3 – Método**: Aqui se apresentam os métodos de pesquisa científica utilizados na elaboração do trabalho, delimitações do problema e os cronogramas referentes a cada capítulo e produções.

- **Capítulo 4 – Análise da aplicação de métodos forense para ambientes corporativos:** O capítulo 4 tem por objetivo o estudo dos tipos de estratégias de investigação forense, as técnicas e ferramentas disponíveis para a execução de tais técnicas, a fim de se embasar a definição do modelo proposto por este trabalho.

- **Capítulo 5 – Modelo conceitual:** O capítulo 5 se beneficia do que foi levantado nos capítulos 2 e 4 com a apresentação dos conceitos de segurança e forense, e propõe um modelo conceitual de investigação forense a ser posto em prática para a validação deste trabalho.

- **Capítulo 6 – Execução do modelo em estudo de caso:** Aqui se aplica o modelo conceitual proposto no capítulo 5 em um estudo de caso empírico elaborado pelo autor, se tratando de um vazamento de informação via *e-mail* de um módulo de *software* para a concorrente.

- **Capítulo 7 – Conclusão:** O capítulo 7 apresenta todas as conclusões tiradas da execução do modelo, das possíveis variações que uma investigação pode produzir, e apresenta o que o autor estabelece como trabalhos futuros.

A divisão em 7 capítulos se dá pela complexidade do tema, em proporção à quantidade de conceitos e pré-conceitos necessários para que se entenda a aplicação de segurança da informação e métodos investigativos em conjunto em prol da elaboração de um modelo final como proposta, inviabilizando a formatação tradicional de somente 5 capítulos.

2 REVISÃO BIBLIOGRÁFICA

Este capítulo tem como foco a contextualização do termo “informação” no meio digital, bem como apresentar a teoria e importância real da segurança e gestão de informação para ambientes corporativos e pessoais, de modo a ilustrar as práticas comuns abordadas no meio digital para que seja possível e viável a proteção de informação trafegada em rede.

2.1 INFORMAÇÃO

Do ponto de vista dos vestígios, existem várias formas de classifica-los por tipos, mas, de um modo geral, eles podem ser (NEW YORK Computer Forensic Services, 2011 *apud* MADEIRA, 2012):

- **Dados ativos –** são aqueles que podem ser prontamente vistos, como arquivos de texto e imagens, programas e arquivos usados pelo sistema operacional. São os tipos de dados mais fáceis de serem extraídos. (MADEIRA, 2012, p.15).

- **Dados arquivados –** são aqueles que foram alvo de *backup*. Podem ser CD-ROM, DVD, fitas magnéticas, discos rígidos. (MADEIRA, 2012, p.15)

.

- **Dados latentes –** são aqueles que geralmente necessitam de ferramentas especializadas para permitir seu acesso, como dados deletados, parcialmente sobrescritos, cifrados etc. (MADEIRA, 2012, p.15).

Segundo Tálamo e Smit (2007), o avanço da informação no último século é inegável, porém sua consolidação como campo científico, como “Ciência da Informação” tem encontrado alguns obstáculos, e os esforços para identificar o domínio esbarram em algumas

terminologias que indicam diferentes momentos históricos da produção de conhecimento no ramo.

Segundo Lyra (2008), a informação é um bem de grande valor para os processos de negócios da organização, mas também se deve considerar a tecnologia, o meio que a suporta, e que permite que ela exista, e das pessoas que a manipulam no ambiente em que a informação está inserida.

Sendo possível ainda mais uma opinião, Laureano e Moraes (2005) citam Rezende e Abreu (2000), dizendo que informação é o dado com uma interpretação lógica ou natural agregada pelo usuário.

Para uma visão mais técnica do assunto, pode-se encontrar que "a informação é o ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e, consequentemente, necessita ser adequadamente protegido" (NBR ISO/IEC 17799, 2005).

Pode-se então observar uma concordância entre autores a respeito da importância da informação em uma organização, e também paralelamente, a importância de sua proteção como bem mais valioso dos dias de hoje, em uma visão de negócios.

Interessante utilizar estes pontos de vista para apontar que nem em todos os casos, a informação é tratada com tal importância, partindo desta afirmação, Boran (1996) e Wadlow (2000) classificam a informação em níveis diferentes de prioridade, respeitando a necessidade de cada empresa assim como a importância da classe de informação para a manutenção das atividades da empresa, sendo estes níveis apresentados como:

- **Pública**. Uma informação que pode vir a público sem maiores consequências danosas ao funcionamento normal da empresa, são informações cuja integridade não é vital.

- **Interna**. Deve-se evitar acesso livre a este tipo de informação, embora as consequências do uso não autorizado não sejam sérias demais. Porém sua integridade é importante, mesmo que não vital.

- **Confidencial**. Informação restrita aos limites da empresa, cuja divulgação ou perda pode levar a desequilíbrio operacional, e eventualmente perdas financeiras ou de confiabilidade perante um cliente externo.

- **Secreta**. Informação crítica para as atividades da empresa, cuja integridade deve ser preservada a qualquer custo e cujo acesso deve ser restrito a um número reduzido de pessoas. A segurança desse tipo de informação é vital para a organização.

Independente da relevância ou do tipo da informação, a gestão dos dados organizacionais é estratégica porque possibilita a tomada de decisões em qualquer âmbito institucional (LAUREANO; MORAES, 2005).

2.1.1 Ativo da Informação

Ativo de informação é qualquer coisa que tenha valor para a organização (NBR ISO/IEC 27001, 2006).

Quebrando este conceito para uma representação mais específica, de modo a exemplificar os ativos da informação, a norma NBR ISO/IEC 17799:2005 define como ativo de informação, bancos de dados, documentação de sistemas, planos de continuidade, material de treinamento, informações arquivadas, etc.

Já Campos (2005) apresenta os ativos de informação de várias outras maneiras, como as próprias pessoas, que utilizam essas informações, todas as tecnologias que suportam a informação, como papel, correio eletrônico, editores de texto, rádio, televisão, telefone, também podendo ser representados pelos processos que suportam o uso da informação, norma para contratação de pessoal, maneiras de utilização de correio eletrônico, de internet, dentre outras variações.

Agora, Lyra (2008) em concordância com outros autores, diz que o ativo da informação é composto pela informação, e tudo aquilo que a suporta ou se utiliza dela.

A partir destas constatações sobre os ativos e a indiscutível convergência de opiniões e conclusões, pode-se observar em suma, que um ativo é tudo aquilo que suporta, ou utiliza a informação, de modo a representar, ou agregar um valor para a informação de modo a deter uma relevância para a organização.

2.2 SEGURANÇA DA INFORMAÇÃO

Uma vez compreendida a importância da informação para as organizações, é necessário entender o que vem a ser a segurança da informação e, ainda, estabelecer uma relação entre a segurança da informação e sua relevância para os negócios da organização (CAMPOS, 2007).

Com a informação assumindo tal grau de importância nas organizações, seguindo o conceito de Caruso (1999), não há hoje organizações humanas que não depende de tecnologia da informação, em maior ou menor grau, de forma que o comprometimento do sistema de informações por problemas de segurança pode causar grandes prejuízos ou mesmo levar a organização à falência.

Hoje em dia, ainda existe uma dificuldade grande por parte das organizações de entender a importância de segurança da informação. A segurança ainda é um campo relativamente novo, muitas empresas ainda não conseguem enxergar sua importância, imaginando apenas que as soluções são caras e não trazem nenhum retorno financeiro, não dando importância às consequências que a falta desta segurança poderá trazer para a empresa. (ALVES, André; ALVES, Fabrício, 2009).

Seguindo o exposto por Spanceski (2004) este segue como o maior desafio da segurança, pois, uma solução de segurança é geralmente imensurável e não resulta em melhorias nas quais todos podem notar que alguma coisa foi feita, sendo que a intenção principal da segurança é justamente que o usuário não perceba nada de errado em sua aplicação.

Por isso, segurança da informação é um assunto amplamente discutido nos dias de hoje, e segundo o exposto por Lyra (2008), em conjunto com o exposto pela norma NBR ISO/IEC 27001:2006, e também pelo exposto na obra de Campos (2007), dentre muitos outros autores, segurança se baseia e se fundamenta por três conceitos, sendo eles; **Confidencialidade, Disponibilidade, e Integridade**.

2.2.1 Confidencialidade

Para Lyra (2008), confidencialidade é a capacidade de um sistema de permitir que alguns usuários acessem determinadas informações ao mesmo tempo em que impede que outros usuários que não estejam autorizados, possam acessar ou apenas visualizar tais informações.

A norma NBR ISO 27001:2006, também apresenta um conceito parecido, quando diz que confidencialidade se dá pela propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados.

Campos (2007) expõe que quando uma informação é acessada por pessoa não autorizada, intencionalmente ou não, seja pela descoberta de uma senha, pelo acesso a documentos ou de qualquer outro modo, então isto é um incidente de segurança da informação por quebra de confidencialidade.

A norma NBR ISO 27001:2006 classifica um incidente de segurança da informação como um simples ou uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação.

Partindo do exposto, pode-se então, resumir confidencialidade como simplesmente a restrição do acesso a informação somente para usuários autorizados para tanto. Sendo para visualização, ou edição.

2.2.2 Integridade

Laureano e Moraes (2005) entendem por integridade, a recuperação da informação (desde que respeitado o conceito de confidencialidade) na sua forma original, sem quaisquer adulterações ou perdas no processo.

Campos (2007) concorda com Laureano e Moraes (2005) porém completa a afirmação, afirmando que quando a informação é inevitavelmente alterada, com ou sem a intenção desse fim, ou por falsificação, interceptação, alteração de um determinado registro

em base de dados, ocorre então, um incidente de segurança da informação, por quebra de integridade.

Então, conclui-se que a integridade da informação é garantida quando a informação está inalterada, correta, verdadeira, e sem nenhum tipo de corrupção para determinado fim.

Porém, ao se falar em integridade, Laureano e Moraes (2005) lembram que outros autores, como Lyra (2008) e Campos (2007) acrescentam outras propriedades quanto a integridade da informação, tais como:

2.2.2.1 Autenticação

Por autenticação de usuário tem-se o procedimento de “garantir que um usuário é de fato quem alega ser” (LYRA, 2008).

Laureano e Moraes (2005) completam essa afirmação, dizendo que não somente o usuário, mas a informação também necessita ser de fato, o que o usuário buscou, ou acessou, para que não viole nenhuma das propriedades expostas anteriormente neste trabalho.

2.2.2.2 Não Repúdio

De forma resumida, Lyra (2008) apresenta o não repúdio apenas como a capacidade do sistema de provar que um usuário realizou de fato, uma determinada ação.

Em outras palavras Laureano e Moraes (2005) apresentam o não repúdio como a impossibilidade de negar (no sentido de dizer que não foi feito) uma operação ou serviço que modificou ou criou uma informação, ou seja, não é possível negar o envio ou recepção de uma informação ou de algum dado.

Alves e Alves (2009) citam Gomes (2006) onde dizem que as assinaturas eletrônicas são eficazes para garantir o não repúdio apenas da origem. No entanto, insuficiente para garantir o não repúdio de recebimento. Diante dessa insuficiência, é preciso algum tipo

de protocolo em que o destinatário ou uma terceira parte confiável envie ao emitente, ou armazene em base confiável, uma mensagem comprobatória do recebimento, sendo que a mensagem de resposta (que é a prova do recebimento) deve ser também assinada eletronicamente.

2.2.2.3 Legalidade

Para essa propriedade, observa-se uma convergência de opiniões e pesquisas entre os autores pesquisados para a realização deste trabalho, sendo elas descritas abaixo.

De forma bastante resumida, Lyra (2008) diz que legalidade é a garantia de que o sistema esteja aderente à legislação pertinente.

Elaborando o texto, Laureano e Moraes (2005) entendem por legalidade a aderência de um sistema à legislação, e as características das informações que possuem valor legal dentro de um processo de comunicação, onde todos os ativos estão de acordo com as cláusulas contratuais pactuadas ou a legislação nacional ou internacional vigente.

2.2.2.4 Privacidade

Foge do aspecto de confidencialidade, pois uma informação pode ser considerada confidencial, mas não privada. Uma informação privada deve poder ser vista/ lida/ alterada somente pelo seu dono. Garante ainda, que a informação não será disponibilizada para outras pessoas (neste caso é atribuído o caráter de confidencialidade à informação). É a capacidade de um usuário realizar ações em um sistema sem que seja identificado. (LAUREANO; MORAES, 2005).

Capacidade de um sistema de manter anônimo um usuário, impossibilitando o relacionamento entre o usuário e suas ações (por exemplo, o sistema de voto eletrônico). (LYRA, 2008).

Analisando as duas citações, percebe-se uma divergência de áreas abordadas, enquanto Lyra (2008) aborda as ações, e o âmbito do usuário, Laureano e Moraes (2005) preferem abordar a informação em si, e as ações atribuídas à sua manipulação.

2.2.2.5 Auditoria

Laureano e Moraes (2005) entendem por auditoria, a rastreabilidade dos diversos passos de um negócio e processo, identificando os participantes, os locais e horários de cada etapa, aumentando a credibilidade da organização, além de adequá-la às políticas legais e internas.

Agora, de uma maneira mais elaborada e técnica, Alves e Alves (2009) explicam auditoria como a gravação, armazenamento e análise de informações importantes, que são capazes de determinar quais ações relevantes à segurança ocorreram e quem as cometeu.

Gomes (2006) completa dizendo que é importante a criação de um mecanismo automático para detecção de problemas. Sendo estes: alarmes e respostas automáticas a uma tentativa de invasão. Pois permitem, que detectada uma situação suspeita, o sistema envie um *e-mail*, por exemplo, apresente uma mensagem “logada” via console para o *admin*, ou tome alguma medida de auto-proteção.

2.2.3 Disponibilidade

Propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada (NBR ISO/IEC 27001, 2006).

Lyra (2008) completa este conceito, dizendo que toda a informação deve estar disponível para todos que precisarem dela para a realização dos objetivos empresariais.

Então, conclui-se que a propriedade da disponibilidade da informação consiste na recuperação da informação em sua forma original (para que não seja violada a propriedade de integridade), somente por usuários autorizados (para que não ocorra incidente de segurança da

informação por quebra de confidencialidade), no momento em que tal usuário precise acessá-la e/ou alterá-la de alguma forma.

2.2.4 Vulnerabilidade

Os ativos de informação possuem vulnerabilidade ou fraquezas que podem gerar, intencionalmente ou não, a indisponibilidade, a quebra de confidencialidade ou integridade. A vulnerabilidade de um ativo é o seu ponto fraco. (LYRA, 2008).

Entretanto nem toda vulnerabilidade é explorada, Lyra (2008) também explica essa informação quando diz que as vulnerabilidades podem ser exploradas, ou não, dependendo da necessidade da quebra de segurança, ou da importância do ativo, ou da informação em si, porém, é de grande importância que as vulnerabilidades de um ativo sejam devidamente levantadas e prevenidas.

2.2.5 Ameaças

Para Campos (2007), a ameaça é um agente externo ao ativo de informação, que se aproveitando de suas vulnerabilidades pode quebrar a confidencialidade, integridade ou disponibilidade da informação, quebrando as propriedades da segurança, causando um incidente, e por consequência, podendo causar danos à organização.

Carvalho (2005) não se prende ao conceito de agente externo concreto, mas exalta a ameaça como a situação iminente de invasão a um sistema de informação, frisando que se um ativo se dá por vulnerável, está ameaçado a todo o tempo, mesmo que não revelada uma ameaça concreta, ela existe.

Lyra (2008) também fala deste tópico como um ataque em potencial ao ativo de informação, por um agente externo real, que pode quebrar as propriedades da segurança da informação e capturar dados e informações recorrentes ao seu objetivo.

Campos (2007) ainda completa o conceito, observando que agentes naturais também podem ser ameaças a um sistema de informação, como tempestades elétricas, enchentes ou incêndios, mas sem descartar as ameaças óbvias de vírus, *spywares*, *worms*, entre outros.

2.2.5.1 Ataques

Ataques são tipos de incidentes de segurança caracterizados pela existência de um agente que busca obter algum tipo de retorno, sendo financeiro ou pessoal, atingindo algum ativo de valor (valor este podendo variar de moral, até financeiro), como diz Lyra (2008).

Por exemplo, se um vírus explora a vulnerabilidade de um servidor de serviços *WEB*, deixando-o inoperante ou indisponível, isto gera um prejuízo ou um impacto para a organização (CAMPOS, 2007).

Já Carvalho (2005) discorre sobre ataques como sendo os métodos utilizados por atacantes para invadir ou danificar um sistema de informação, se fazendo possível a recuperação, interceptação, ou até mesmo destruição de determinada informação, ou determinado dado.

Uma vez explicado de forma geral o que representa um ataque, se faz útil e necessário exemplificar alguns dos ataques mais comuns encontrados hoje.

2.2.5.2 Tipos de ataque.

Existem muitos tipos de ataques a sistemas de informação, e ativos de informação, sua variedade vem em proporção a variedade de sistemas e métodos de comunicação de informação, logo, controlar um sistema de informação vêm sendo cada vez mais primordial, e essencial no mais alto nível, em organizações, como dito por Carvalho (2005).

A seguir neste trabalho, são listados os principais tipos de ataques que preocupam as organizações em geral, bem como uma breve descrição de cada um, entendendo a importância e o dano que cada um pode causar.

2.2.5.2.1 Ataque físico

Aqui, a palavra "físico" abstrai do meio *software* ou do meio de redes de computador, então, é seguro dizer que ataques físicos acontecem diretamente ao *hardware* por meio de roubos de CDs, HDs, fitas magnéticas, dentre outros, baseando-se nas palavras de Lyra (2008).

Além disso, a norma NBR ISO/IEC 17799:2003 cita brevemente esta constatação, ao levantar a questão de muros, cercas e trancas em ambientes onde estão instalados equipamentos que contém quaisquer tipos de informações dentro de uma organização, o chamado "perímetro" citado por essa norma.

A definição clara do perímetro de segurança ajuda a estabelecer melhor os investimentos e definir que tipos de barreiras são mais adequados para a proteção do ativo da informação (LYRA, 2008).

Com isso em mente, pode se ter uma ideia de que prédios (*mainframes*), geradores de energia, cofres, podem ser grandes alvos em potencial de ataques físicos, sendo mais indicado portanto, baseando-se no exposto anteriormente neste tópico, que um perímetro físico de segurança seja estabelecido.

2.2.5.2.2 Packet sniffing

Packet Sniffing é um método de ataque que "toca" cada pacote, conforme os mesmos trafegam pela rede, ou seja, é uma técnica utilizada para interceptar e acessar informações que "pertencem" a outros usuários da rede. *Packet Sniffers* podem operar como

uma ferramenta administrativa, ou para propósitos maliciosos, dependendo das intenções do atacante que está utilizando deste meio de ataque. (SUHAIL et.Al, 2003 – Tradução nossa).

Carvalho (2005) reforça este conceito, dizendo que os serviços de FTP (*File Transfer Protocol*) são os mais vulneráveis a este tipo de ataque, pois é possível obter facilmente as senhas dos usuários que utilizam esses serviços.

Além disso, Carvalho (2005) também comenta que *Packet Sniffing* é um ataque de fácil execução, e que pode ser usado por qualquer um que possua conhecimentos mínimos em computação, pois existem *softwares*, que são de utilização simples e produzem bons resultados

2.2.5.2.3 Port scanning

Utilizando e as ideias de Urupoj et. Al (2002) um ataque do tipo *Port Scanning* é um método para descobrir falhas exploráveis em canais de comunicação que vêm sido utilizados por um bom tempo. A ideia chave é sondar as portas de rede e guardar informações úteis para um ataque. Em alguns pontos de vista, *Port Scanning* não é considerado como uma invasão de rede, mas é considerado como um método de descobrir possibilidade de se aproveitar do sistema para um ataque.

Carvalho (2005) reforça essa constatação, dizendo mais resumidamente, que um *Port Scanning* consiste na análise de um sistema com o intuito de descobrir os serviços que estão disponíveis no mesmo, através da análise das portas TCP (*Transmission Control Protocol*) e UDP (*User Datagram Protocol*).

E de posse das informações obtidas através desse tipo de ataque, pode-se concentrar esforços para comprometer recursos específicos.

2.2.5.2.4 Scanning de vulnerabilidades

Como visto anteriormente, um *Port Scanner* é capaz de identificar as portas e serviços disponíveis em um sistema computacional, mas essas informações ainda não são suficientes para comprometer totalmente a segurança de um sistema.

Para isso, Lyra (2008) e Carvalho (2005) dizem que precisa-se encontrar alguma vulnerabilidade nessas portas e serviços, tarefa essa, do *Scanning* de vulnerabilidades.

Que são, ainda de acordo com o dito por esses dois autores, *softwares* que executam uma série de testes na rede de computadores a ser atacada, procurando por falhas de segurança em serviços, protocolos, aplicativos e sistemas operacionais.

Ainda salientam, que os mais comuns tipos de vulnerabilidades encontradas pelos *scanners* de vulnerabilidades são em compartilhamento de arquivos (sem o uso de senhas), configurações incorretas dos sistemas e *softwares* desatualizados.

2.2.5.2.5 Denial of service

O relatório técnico de Schuba et al. (1996) mostra que o *Denial of Service*, também conhecidos como *SVN Flooding*, funciona com um atacante enviando muitas requisições de conexão TCP com origem falsificada, direcionadas diretamente ao computador da vítima, ou organização. Cada requisição causa o *host* (equipamentos que abrigam sistemas computacionais, normalmente computadores pessoais ou servidores) alvo a instanciar estruturas de dados a partir de um *pool* de recursos já limitado.

Uma vez que os recursos do *host* alvo são exauridos, mais nenhuma conexão TCP pode ser estabelecida, assim, negando o serviço. (SCHUBA et. Al, 1996).

Carvalho (2005) observa que além dos *Denial of Service* (DoS), também existem os ataques do tipo DdoS (*Distributed Denial of Service*), que são os ataques coordenados, onde diversos *hosts* são controlados e configurados por um atacante de forma a efetuarem ataques simultâneos contra um determinado alvo.

2.2.5.2.6 Ataques a nível de aplicação

Carvalho (2005) explica os ataques a nível de aplicação, como ataques que envolvem basicamente a exploração de vulnerabilidade em aplicativos e protocolos na camada de aplicação da pilha de protocolos TCP/IP (*Transmission Control Protocol/ Internet Protocol)*, isto é, a camada mais próxima do usuário.

Ainda utilizando o conceito de Carvalho (2005), fazem parte deste tipo de ataque:

- ***Buffer overflow:*** Método de ataque no qual o *hacker* explora falhas de implementação envolvendo o controle de *buffer* (memória temporária para armazenamento de dados).

- ***Navegadores:*** Falhas de segurança nos *browsers* (software que normalmente é utilizado para visualizar páginas na *Web*) são explorados de forma que o atacante possa invadir o sistema.

- **Vírus:** Programa capaz de infectar (fazer cópia de si mesmo) outros programas e arquivos.

- ***Worm:*** Programa capaz de se propagar automaticamente através de redes de computadores (enviando cópias de si mesmo para outros computadores), que diferentemente do vírus, não precisa ser explicitamente executado para funcionar.

- **Cavalo de tróia (*Trojan horse*):** Programa que executa funções normalmente maliciosas sem que o usuário tome conhecimento.

A fim de manter o fluxo deste trabalho, após conhecer os tipos de ataques, resta conhecer os atacantes que irão de fato fazer uso do exposto até aqui.

2.2.5.3 Atacantes

Dá-se o nome de atacante à pessoa que realiza um ataque (tentativa de comprometimento ou invasão) a um sistema computacional, obtendo êxito ou não. (CARVALHO, 2005).

Com a variedade de sistemas de informação presentes nos dias de hoje, sendo pessoais ou corporativos, é primordial conhecer mais detalhadamente cada atacante, sua área de atuação, e preferência de invasão a determinado sistema, dessa forma entende-se melhor as ameaças que cada tipo de atacante pode trazer a um sistema.

2.2.5.3.1 Script Kiddies

Hackers experientes sabem como encobrir suas ações, agora, os menos experientes e menos habilidosos, como os *scripts kiddies*, não tem essa habilidade e traço, devido a seu pouco conhecimento de informática e sistemas de informações, e normalmente dependem de *hackers* mais experientes para automatizar suas invasões. (ARBAUGH *et. Al* 2000 – Tradução nossa).

Carvalho (2005) concorda com Arbaugh et.Al (2000) dizendo que os *Script Kiddies* são de fato, conhecidos pelo baixo conhecimento técnico e por usarem ferramentas disponíveis na internet para invadir sistemas, e que são uma ameaça mais comumente enfrentada pelas empresas, pois são a maioria dos atacantes existentes hoje. Não possuem um alvo específico, podendo atacar qualquer tipo de organização que possua comunicação com a internet.

2.2.5.3.2 Crackers

Os crackers são pessoas aficionadas por informática que utilizam seu grande conhecimento na área para quebrar códigos de segurança, senhas de acesso a redes e códigos de programas com fins criminosos. (MARTINS, 2012).

Carvalho (2005) concorda com Martins (2012) neste aspecto, dizendo que diferentemente dos *Script Kiddies*, os *Crackers* possuem conhecimento avançado em informática, são capazes de quebrar proteções de sistemas e *softwares*, além de roubar informações importantes e destruir os sistemas invadidos, sendo então responsáveis pela maioria dos crimes virtuais destaques em jornais e revistas.

A relação com os *Crackers* e o termo pirata virtual, fica evidente com a expressão popular de programas "crackeados", ou seja, programas piratas, com chaves falsas que simulam um serviço "original" porém falsificado digitalmente.

2.2.5.3.3 Carders

Carvalho (2005) cita Spy (2001) quando diz que *hackers* do tipo *carder* são responsáveis por efetuar compras através da internet, usando cartões de crédito, daí o nome *carder*. Ainda diz que quando se faz uma compra na internet utilizando cartões, está se fazendo referência ao número e validade dos mesmos e não fisicamente, portanto são apenas os números que são roubados ou gerados por *softwares* específicos para esse fim.

2.2.5.3.4 Cyberpunks

Cavallaro (2000) em sua obra sobre os *Cyberpunks* explica que são tipos de *Crackers* que detém um grande conhecimento de informática, e sendo assim, podem causar grander danos a um sistema, ou organização.

Cavallaro (2000) também observa algo interessante, dizendo que os *Cyberpunks* nasceram na geração digital, e seu contato constante com a tecnologia ajudaram em muito na sua vasta área de conhecimento, diz também, que a influência da ficção científica também contribuiu para que esse tipo de *Cracker* surgisse "no mercado", como um grande perigo, devido, claro, a já mencionada habilidade em informática.

2.2.5.3.5 Insiders

Atribui-se, geralmente, aos *Insiders* a execução de espionagem industrial. Eles são funcionários e ex-funcionários da própria empresa alvo, e normalmente, os maiores prejuízos resultados de um ataque vêm deste atacante, justamente por conhecerem os caminhos de dentro da empresa, facilitando a interceptação de dados importantes, e muitas vezes vitais para a organização. (CARVALHO, 2005).

2.2.5.3.6 Coders

Como o nome já diz, os *Coders* constroem sistemas, escrevem livros, e compartilham seus conhecimentos. Como Kevin Mitnick, *hacker* que cumpriu pena por atos criminosos através da utilização de computadores. Hoje, impedido pela justiça de utilizar computadores e trabalhar como consultor técnico, é muito requisitado para proferir palestras sobre segurança, lembra Carvalho (2005).

O prório Kevin Mitnick escreveu um livro chamado *The Art of Deception* onde descreve os objetivos dos *Hackers* em geral, como utilizar engenharia social para capturar informação, e como se aproveitar das falhas humanas para conseguir um "prêmio", ou objetivo, em um ataque a ativo de informação.

2.2.5.3.7 White Hats

"*White Hats*" são aqueles *Hackers* que usam suas habilidades de forma que pode ser definida claramente como ética e correta. (PASHEL, 2008 – Tradução nossa).

Exemplos disso, são funcionários que, com permissão, atacam a rede de uma organização para que sejam descobertas falhas, e também para que possam ajudar agências de segurança, e serviços de inteligência, de modo a solucionar crimes. É parte do dever dos *White Hats* utilizar seus conhecimentos de modo a beneficiar outras pessoas (FALK, 2005 *apud* PASHEL, 2008 – Tradução nossa).

2.2.5.3.8 Black Hats

Apenas pelo título, pode-se observar que os *Black Hats* são o oposto dos *White Hats*, visto o que foi dito anteriormente, se os *White Hats* são *Hackers* que utilizam seu conhecimento para o bem de outros, e de organizações, os *Black Hats* por consequência, utilizam seus conhecimentos para causar danos, e perdas para pessoas e organizações.

Carvalho (2005) exemplifica isso dizendo que utilizam seus conhecimentos para invadir os sistemas de organizações para roubar informações, de forma a obter retorno financeiro vendendo-as ou chantageando a organização invadida. A prática de chantagem utilizada por esse tipo de *Hacker* é conhecida como *blackmail*, e também pode-se observar que normalmente, qualquer ação que tem por objetivo a danificação de um sistema, ou causar algum prejuízo, é atribuída aos *Black Hats*.

2.2.5.3.9 Gray Hats

A natureza ética de um *Gray Hat* é, como o nome sugere, uma área "cinzenta" de atuação. Se classificam como *Gray Hat Hackers,* os chamados justiceiros (indivíduos que utilizam seus conhecimentos de informática para investigar e punir/incriminar criminosos soltos por aí). (PASHEL, 2008 – Tradução nossa).

Importante observar, que por melhor que sejam as intenções, os *Gray Hats Hackers* ainda atuam fora da lei, por isso, não são considerados *White Hats*, e nem *Black Hats*, mas uma espécie de fusão entre ambos. (FALK, 2005 *apud* PASHEL, 2008 – Tradução nossa).

2.2.5.3.10 Phreackers

Com base no dito por Carvalho (2005), eles são os *Hackers* da telefonia, responsáveis por fraudes telefônicas, tais como alteração de contas, ataques às centrais telefônicas e realização de ligações gratuitas.

Atualmente com o advento dos *smartphones*, estes se tornam o grande alvo dos *Phreackers* visto que a maioria das informações pessoais de uma pessoa agora se encontram em seus bolsos, como dados de redes sociais, bancários, contatos, etc.

2.2.6 Criptografia

A proliferação dos computadores e sistemas de comunicação na década de 60 trouxe consigo uma demanda de proteção de dados tanto dos sistemas e setores privados, quanto pessoais por serviços de segurança de fluxo de informação. (MENEZES; OORSCHOT; VANSTONE, 1996 – Tradução nossa).

A criptografia é a ciência de transformar dados que aparentemente podem ser entendidos e interpretados pelas pessoas, em dados que não possuem significado algum, e que quando necessário podem ser recuperados à sua forma original. (CARVALHO, 2005).

Ou seja, criptografia tem por objetivo ocultar (codificar) informações de uma certa relevância, de modo a dificultar a leitura da mesma, e assim, prevenir que determinado dado, ou informação seja acessada e utilizada por não autorizados.

Criptografia possui algumas terminologias básicas que formam o embasamento da ciência, como: (STALLINGS, 2002).

- ***Plaintext*** (Texto plano/limpo) consiste na informação original, em texto legível, sem alterações de qualquer modo, como explicado por Carvalho (2005).

- ***Ciphertext*** (Texto cifrado) mensagem codificada, apresentada após a aplicação de determinado método, ou algoritmo de encriptação. (STALLINGS, 2002 – Tradução nossa).

- ***Cipher*** (Cifra) Martini (2001) apresenta a cifra como o algoritmo de codificação aplicado ao *plaintext* de modo a transformá-lo em *ciphertext*..

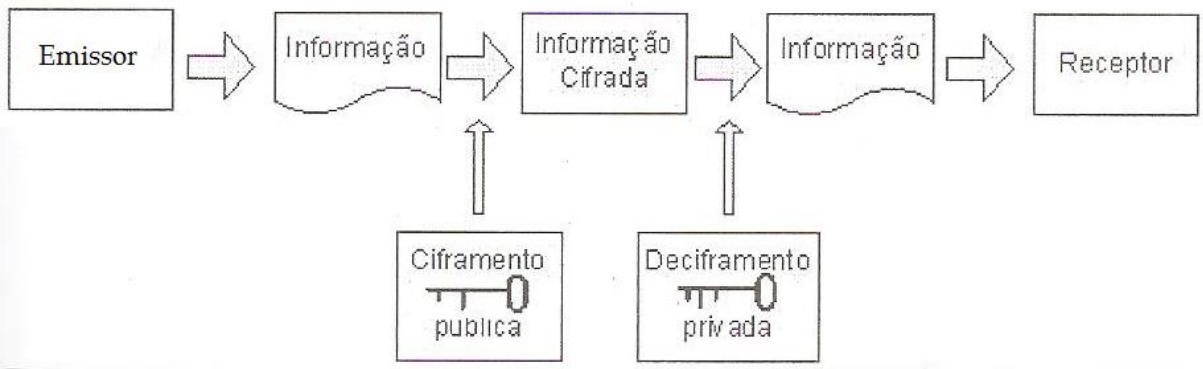
- ***Key*** (Chave) Segundo Menezes, Oorschot e Vanstone (1996) as chaves podem ter algumas classificações, mas em suma, uma chave é o essencial para a encriptação, e decriptação de um *plaintext*, como um pedaço de informação, que determina a entrada e saída de dados funcional de um algoritmo de encriptação/decriptação.

- ***Encipher*** ou ***Encrypt*** (Encriptação, ou codificar) Menezes, Oorschot e Vanstone (1996) dizem, assim como Carvalho (2005), que a encriptação é a utilização de uma chave, em conjunto com um algoritmo de encriptação, para codificar uma entrada (*plaintext*) para produzir um *ciphertext*, ou texto cifrado, criptografado.

- ***Decipher*** ou ***Decrypt*** (Decriptação, ou Decodificar) Carvalho (2005) brevemente descreve este processo como o oposto da encriptação, também utilizando uma chave e um algoritmo, para que o *ciphertext* se torne novamente o *plaintext* pretendido.

Existem basicamente três sistemas criptográficos para cifrar dados: criptossistemas simétricos, criptossistemas assimétricos e criptossistemas híbridos, que possuem um esquema de funcionamento apresentado na figura 2.

Figura 2 - Esquema de funcionamento de criptossistemas



Fonte: (CARVALHO, 2005, p.38)

Martini (2001) expõe a importância de conhecer os tipos de criptossistemas existentes no âmbito da criptografia, visto que qualquer criptossistema deve garantir que as mensagens que trafegam num canal de comunicação qualquer devem ter a privacidade, a integridade e a autenticação garantidas.

Oliveira (2007), diz que um criptossistema é um conjunto de técnicas, e características que constituem o processo de encriptação e decriptação de informação, onde se descrevem como a informação sofre sua transformação, quais os caminhos, e quais os processos que levam a informação a ser cifrada e vice-versa.

2.2.6.1 Criptossistemas Simétricos

Martini (2001) em concordância com o exposto por Carvalho (2005), diz que criptossistemas simétricos são utilizados para criptografar uma informação, ou para decifrar uma informação, fazendo uso de um algoritmo de criptografia que utiliza apenas uma chave criptográfica, isto é, a mesma chave utilizada para encriptar o *plaintext* é utilizada para decriptar o *cipher text*.

De forma mais resumida, Oliveira (2007) explica criptossistemas simétricos como apenas sistemas onde dada uma chave é possível manipular a encriptação da informação.

2.2.6.2 Criptossistemas Assimétricos

Oliveira (2007), Lyra (2008) e Carvalho (2005) descrevem criptossistemas assimétricos de maneira semelhante, e diferente ao mesmo tempo.

Oliveira (2007) é mais direto quanto ao assunto, dizendo apenas que criptossistemas assimétricos são criptossistemas que utilizam duas chaves distintas para funções distintas de encriptação ou decriptação.

Lyra (2008) e Carvalho (2005), se aprofundam um pouco mais no assunto, e em concordância dizem que a diferença entre sistemas simétricos e assimétricos é realmente o uso de uma ou duas chaves de encriptação, mas também observam que o processo só é possível em um caminho ou outro se estiver em posse das duas chaves.

Carvalho (2005) continua sobre o assunto, dizendo que os sistemas de chaves públicas partem do princípio de que cada pessoa interessada em transmitir ou receber informações criptografadas possua um par de chaves, uma chave chamada de chave pública e a outra, uma chave privada, onde a chave pública é conhecida por todos, ou seja, é amplamente divulgada, ao passo que a chave privada deve ser conhecida somente pelo usuário detentor de tal informação.

Com os conceitos apresentados, pode-se levantar vantagens e desvantagens ao se utilizar este criptossistema, sendo a vantagem, o fato da chave privada não precisar ser

transmitida para se trocar informações cifradas, garante que ela não seja interceptada, ou seja, há um aumento notável na segurança.

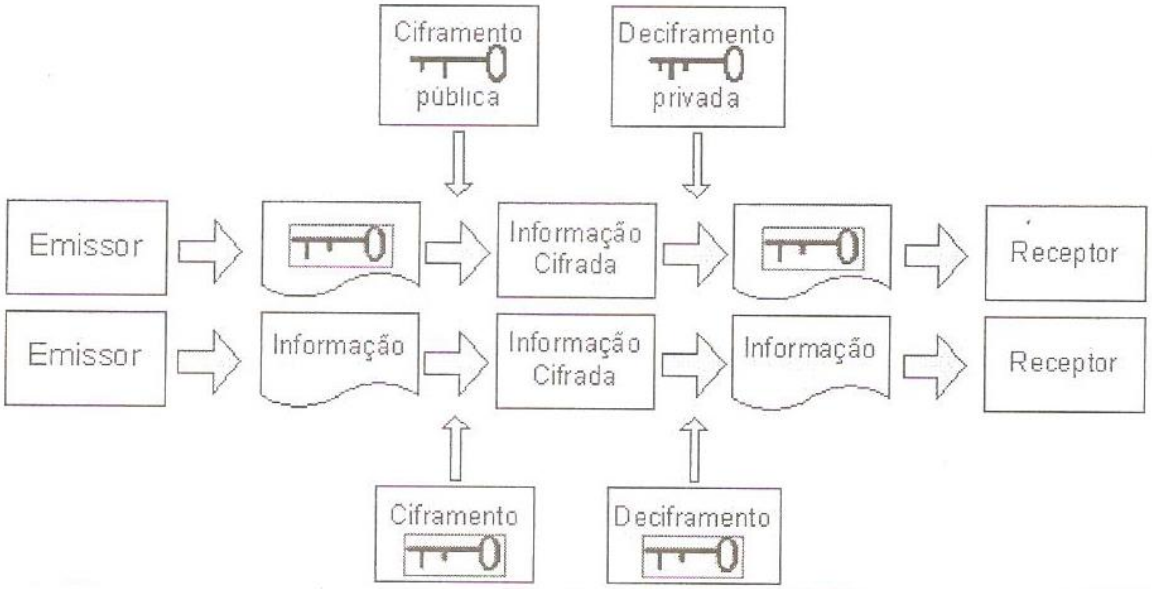
A desvantagem está associada então, ao tempo gasto para se decriptar uma informação cifrada por criptossistema assimétrico, tendendo a ser mais demorado justamente pela presença de duas chaves.

2.2.6.3 Criptossistemas Híbridos

Como o nome já sugere, criptossistemas híbridos são a junção das funções e características dos criptossistemas simétricos e assimétricos para transmitir informações encriptadas.

Carvalho (2005) nos mostra na figura 3, como é representado o fluxo lógico de um criptossistema híbrido.

Figura 3 - Processo de um criptossistema híbrido



Fonte: (CARVALHO, 2005).

Martini (2001), Oliveira (2007) e Carvalho (2005), exaltam que como os algoritmos simétricos são mais rápidos do que os assimétricos, eles são usados para

criptografar as informações (que normalmente possuem tamanhos consideráveis). O problema agora é transmitir de forma segura a chave utilizada para cifrar as informações, fato que justifica a utilização de um algoritmo assimétrico, pois pode-se criptografar a própria chave (que é extremamente pequena em relação às informações em questão, portanto sendo de rápida cifragem mesmo quando se utiliza algoritmos assimétricos), e transmiti-la de forma segura, já que nenhuma chave precisa ser transmitida.

2.2.6.4 Importância da Criptografia

A importância da criptografia é um assunto de convergência entre muitos autores, principalmente após expor os criptossistemas simétricos, assimétricos e híbridos. Além de sua própria definição de codificar informações, a criptografia se mostra importante, para Carvalho (2005), Lyra (2008), Oliveira (2007), Spanceski (2004) e Martini (2001) para garantir todas as propriedades da segurança da informação, de modo a utilizar técnicas, métodos e metodologias, a criptografia é o ponto chave da segurança, já que é a responsável por codificar informação plena para informação segura, cifrada e de acesso restrito a quem possui a chave para decifrar a informação.

Martini (2001) e Carvalho (2005) citam algumas importâncias mais específicas da criptografia, sendo:

- **Assinaturas digitais**: código utilizado para verificar a integridade de uma informação ou mensagem, além de poder ser utilizada para verificar se o remetente de uma mensagem é mesmo quem diz ser, isto é obtido através da utilização de criptossistemas assimétricos.

- **Protocolos de segurança**: diversos protocolos de comunicação fazem uso da criptografia para garantir a segurança dos dados transmitidos, como exemplos podem ser citados o S/MIME (*Secure Multipurpose Internet Mail Extensions*), TLS (*Transport Layer Security*) e o IPSec (*Internet Protocol Security*).

- **Certificados digitais**: um dos elementos utilizados pelos protocolos de segurança que tem como base a criptografia de chaves públicas, contendo informações sobre o seu dono.

- **Redes privadas virtuais (VPN)**: redes privadas que utilizam redes públicas, como a internet, como infraestrutura e que garantem através da criptografia, que apenas usuários autorizados tenham acesso às mesmas.

Pelo exposto até aqui, a criptografia se apresenta como um dos grandes fundamentos da segurança da informação, mas como gerir um sistema de segurança?

2.3 GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Visto os conceitos de informação e segurança, é interessante completar o conteúdo apresentando Gestão, ou Governança da informação.

Com o conceito de Fagundes (2008) a gestão da segurança da informação se traduz no planejamento, execução, monitoramento e na melhoria contínua da Segurança da Informação, ou seja, representa as tarefas diárias que são necessárias para que um programa de segurança da informação seja ativo.

Por exemplo: divulgar e manter a política de segurança da informação, responder e tratar incidentes de segurança, monitorar e corrigir vulnerabilidades, dentre outras atividades.

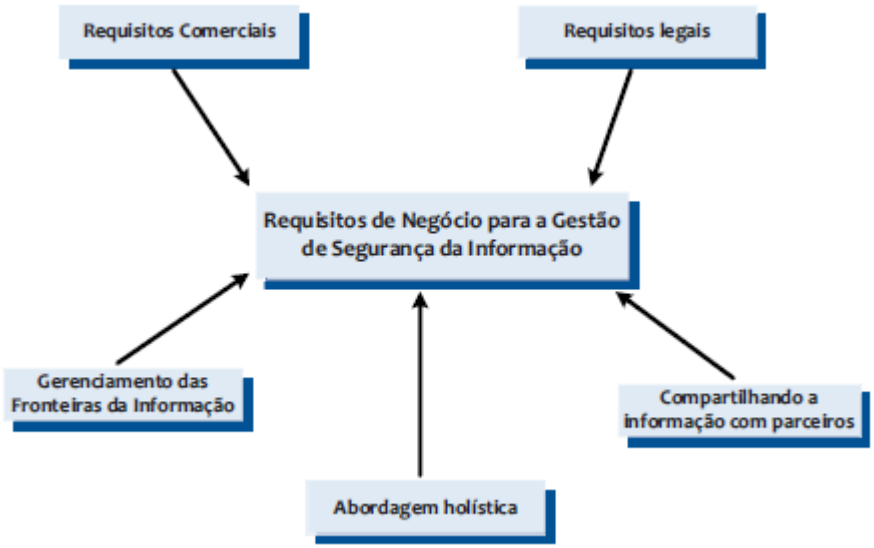
Agora, em contrapartida, também pelo conceito de Fagundes (2008) a Governança da segurança da informação, tem como missão direcionar a gestão da segurança da informação de forma eficaz e transparente alinhada com o negócio e considerando a evolução dos objetivos estratégicos da organização e as tendências do mercado.

2.3.1 Requisitos de Gestão da Segurança da Informação

Conforme o apresentado por Lento (2010) os requisitos de gestão de segurança da informação estão dispostos em cinco componentes, sendo eles, **requisitos comerciais, requisitos legais, compartilhando a informação com parceiros, abordagem holística, e gerenciamento das fronteiras da informação**.

A figura 4 mostra um diagrama desses cinco componentes:

Figura 4 - Componentes dos requisitos de negócio da GeSI



Fonte: (LENTO, 2010, p.109).

Cada um destes componentes conforme visto na figura, compõe os requisitos de negócio para a GeSI, de modo a viabilizar, componentizar e formalizar a implantação da GeSI em uma corporação.

A seguir este trabalho apresenta cada um dos itens citados para que se esclareça mais o processo de composição exposto acima.

2.3.1.1 Requisitos Comerciais

Segundo Lento (2010), os requisitos comerciais tendem a se basear pela relação cliente/*stakeholder*, ou simplesmente, partes interessadas, onde são especificados os requisitos de contrato, como por exemplo, acordos de confidencialidade ou de não divulgação, responsáveis por refletir as necessidades de proteção das informações manipuladas nesse meio.

Além disso, entra também em requisitos comerciais o *marketing*, ou seja, a parte de divulgação de importâncias, vantagens competitivas e o diferencial do produto que é tratado e entregue com segurança.

Observa-se também presente no texto de Lento (2010), as partes de estratégia e tecnologia, que tem por objetivo respectivamente, demonstrar aos parceiros comerciais, clientes e fornecedores o compromisso com a segurança da informação, e possuir uma ferramenta de gestão de segurança da informação que realmente forneça controle e confiança aos seus colaboradores, clientes, etc.

2.3.1.2 Requisitos Legais

Lento (2010) concorda com o exposto por Oliveira (2008), no que diz respeito aos requisitos legais, de ponto à tratarem da mesma forma o aspecto de regulamentos internos, direitos autorais, e regras de uso de recursos.

Ao que diz respeito aos regulamentos internos, ambos autores exaltam que faz parte de um requisito legal, possuir requisitos contratuais, devidamente documentados e que sirvam como referência na criação de normas de segurança.

No campo de direitos autorais, Lento (2010) estabelece que é um requisito legal possuir procedimentos adequados para garantir os requisitos legais, regulamentares e contratuais na garantia da manutenção dos direitos e patentes no que tange à utilização e manipulação de projetos, sistemas, livros e outros tipos de obras e produtos próprios.

O próximo assunto quanto aos requisitos legais é a abordagem de regras de uso de recursos. Segundo Oliveira (2008) o uso de recursos internos de uma organização deve

possuir uma política, ou conjunto de regras ou normas que especifiquem como, e quando utilizar tais recursos.

Embora não exposto por Oliveira (2008), o quesito investigação é parte da obra de Lento (2010), que fala da necessidade de uma organização de possuir regras que estabeleçam poderes investigativos a quem de direito, na ocorrência de um incidente de segurança.

2.3.1.3 Gerenciamento das Fronteiras da Informação

Siqueira (2005) menciona este tópico indiretamente em seu capítulo sobre Sistemas de Informações Organizacionais, ressaltando sistemas de informação interligados de modo que um funcionário possa acessar informações de ums servidor local/privado da organização remotamente, o que vai de encontro ao dito por Lento (2010), onde a gerência das barreiras que compõe os perímetros externos e das conexões com a internet, intranet, extranet e conexões remotas de funcionários fazem parte de uma propriedade do gerenciamento das fronteiras da informação.

Há ainda, segundo Lento (2010), mais duas propriedades cabíveis a esse requisito, sendo elas:

- Gerência de redes de clientes e parceiros e VPNs.
- Gerência dos acordos de nível de serviços (SLAs), contratos, acordos de nível de gerência (SLM) e acordos com terceiros.

A gerência de redes de clientes em encontro com a gerência de acordos de nível de serviço forma uma diretriz de fronteira que possibilita ao gestor ou auditor o maior controle sobre a rede e as informações que circulam sobre ela.

2.3.1.4 Compartilhando a Informação

Sendo esse um requisito bem simples, Lento (2010) descreve brevemente a estrutura de propriedades competentes como:

- **Internas –** Informações que a organização não gostaria que a concorrente soubesse, ou tivesse qualquer tipo de acesso (projetos e planilhas financeiras, por exemplo)
- **Clientes/compradores/fornecedores –** Informações as quais eles gostariam que não fossem divulgadas.
- Outras informações que necessitam ser compartilhadas com outros parceiros.

Esses tipos de informação posam diferentes vulnerabilidades e ameaças à corporação, principalmente em clientes, compradores ou fornecedores, sendo essas informações vitais na construção da definição da área de negócio e atuação da empresa.

2.3.1.5 Abordagem Holística

Finalizando os requisitos, a abordagem holística segundo Lento (2010), se dá pelo uso das boas práticas de gestão de segurança definidas na norma ISO/IEC 27002, também pelo SGSI buscando equilíbrio entre segurança física, lógica e pessoal, e por fim, a segurança da informação deve ser abordada como um processo de gestão, e não como um processo tecnológico.

2.3.2 Sistema de Gestão de Segurança de Informação (SGSI)

Um SGSI é um sistema de gerenciamento utilizado para estabelecer a política e os objetivos da segurança da informação baseado em uma abordagem de análise de risco do negócio, com o intuito de definir, implementar, operar, monitorar, manter e melhorar a segurança da informação. (OLIVEIRA, 2008)

A norma NBR ISO/IEC 27001:2006 estipula que quando uma organização decide estabelecer um SGSI, a própria deve determinar dois pontos importantes:

- A relevância do sistema aos envolvidos diretamente na aplicação, e gestão.
- E seus requisitos, como suas expectativas, sendo explícitas, implícitas ou obrigatórias.

A norma ainda completa, dizendo que a organização deve garantir o alinhamento do SGSI com as estratégias de controle e administração de riscos internos, com as mesmas estratégias e manutenções propostas pelo SGSI.

2.3.3 O SGSI e o ciclo PDCA (*Plan Do Check Act*)

O ciclo PDCA, ciclo de Shewhart ou ciclo de Deming, é um ciclo de desenvolvimento que tem foco na melhoria contínua. O PDCA é dividido em quatro etapas (*Plan, Do, Check, Act*) e é aplicado para se atingir resultados dentro de um SGSI e pode ser utilizado em qualquer empresa de forma a buscar o sucesso nos negócios, independentemente da área de atuação da empresa. O SGSI, como um sistema de gestão que é, faz uso do PDCA. (QUEIROZ, 2012).

A figura 5 trata da ilustração do ciclo PDCA, em análise apresentada por Queiroz (2012).

Figura 5 - O ciclo PDCA

Fonte: QUEIROZ, 2012

Importante destacar que o ciclo PDCA representa também o método de aplicação proposto por este trabalho, melhor detalhado no capítulo 3, seguindo as normas da NBR ISO/IEC 27001:2005.

2.3.4 Requisitos de um SGSI de acordo com o estabelecido pela norma NBR ISO/IEC 27001:2005

A norma NBR ISO/IEC 27001:2005 estabelece os seguintes requisitos para um SGSI em relação ao ciclo PDCA.

2.3.4.1 *Plan* (Planejamento)

Na etapa de planejamento, deve-se definir a política, objetivos, processos e procedimentos relevantes ao gerenciamento de risco, melhorando assim a segurança da informação, provendo resultados em concordância com os objetivos e as políticas globais da organização. Para isso são executadas as etapas que seguem. (LENTO, 2010, p.122).

- Definir o escopo
- Definir a política do SGSI
- Definição da abordagem de análise/avaliação de riscos da organização. Nesta etapa, a metodologia deve ser definida, assim como os critérios para a aceitação de riscos e nível aceitável de risco.
- Identificar os riscos, que envolve:
    - A identificar ativos e seus proprietários
    - Identificar ameaças
    - Identificar vulnerabilidades
    - Identificar impactos que as perdas de confidencialidade, integridade e disponibilidade podem causar aos ativos.
- Analisar e avaliar os riscos, que envolve:
    - Avaliar impacto para o negócio
    - Avaliar probabilidade real de ocorrência de falha
    - Estimar níveis de risco
    - Determinar se os riscos são aceitáveis ou se requerem tratamento
    - Identificar e avaliar as opções para o tratamento de riscos, que pode ser:
        - Aplicar controles apropriados
        - Evitar risco
        - Transferir risco
        - Aceitar o risco de forma objetiva e consciente, desde que satisfaçam claramente às políticas da organização e aos critérios de aceitação de riscos.
- Documentar o processo de análise e avaliação de risco
- Selecionar objetivos de controle e controles para o tratamento de risco
- Obter aprovação da direção para os riscos residuais propostos
- Preparar a Declaração de Aplicabilidade (SoA – *Service oriented Architecture*), que deve conter:
    - Objetivos de controle e controles selecionados e a justificativa para a seleção
    - Objetivos de controle e controles atualmente implementados

- Objetivos de controle e controles excluídos e a justificativa para a sua exclusão.

Fica claro após este levantamento, o número de etapas e normas a se seguir em uma aparentemente simples etapa de planejamento em um ciclo, o que dificulta uma investigação, e planejamento de SGSI em geral, visto que quanto mais normas existem a serem seguidas, mais demorado o processo tende a ser, e, por consequência, mais complexo.

2.3.4.2 *Do* (Executar)

Nesta fase é realizada a implementação e operacionalização da política, controles, processos e procedimentos do SGSI. Para isso, deve-se: (LENTO, 2010, p.124).

- Formular e implementar um plano de tratamento de riscos
- Com o plano pronto, deve-se implementar os controles selecionados e deve-se também buscar uma forma de se medir a eficácia destes controles
- Implementar os programas de conscientização e treinamento
- Gerenciar as operações do SGSI
- Gerenciar os recursos do SGSI
- Implementar procedimentos e outros controles para detecção e resposta de incidentes de segurança da informação.

Após a fase de execução, é preciso monitorar a implementação executada, então o próximo passo é justamente verificar constantemente a execução, como mostrado a seguir.

2.3.4.3 *Check* (Verificar)

Nesta etapa, avalia-se o desempenho dos processos, política, objetivos e a experiência prática, além de se reportarem os resultados ao gerenciamento para a revisão. (LENTO, 2010, p.124).

A seguir, os passos necessários para realizar tal etapa de acordo com a norma NBR ISO/IEC 27001:2005

- Executar procedimentos de monitoramento e análise
- Realizar análises críticas regulares da eficácia do SGSI
- Medir a eficácia dos controles
- Analisar criticamente as análises/avaliações de riscos
- Conduzir auditorias internas do SGSI
- Realizar análise crítica do SGSI pela direção
- Atualizar os planos de segurança da informação levando em consideração os resultados das atividades de monitoramento e análise crítica.
- Registrar toda e qualquer ação que tenha impacto na eficácia ou desempenho do SGSI

Cada passo exposto acima reflete bem o tipo de ciclo aplicado no modelo PDCA utilizando a NBR ISO/IEC 27001:2005 como plataforma de execução de tais passos. Sendo assim, a análise e execução podem andar em conjunto já que um dos passos consiste em atualizar os planos de segurança, o que pode acarretar mais um ciclo do tipo *plan*, que também pode dar origem à outro ciclo *do*, e assim por diante.

2.3.4.4 *Act* (Monitoramento)

Nesta fase, são realizadas ações preventivas e corretivas com base nos resultados da auditoria do SGSI, também deve-se rever o gerenciamento ou outra informação relevante para manter uma melhoria contínua no SGSI. (LENTO, 2010, p.125).

Para isso, seguem as seguintes etapas:

- Implementar as melhorias identificadas no PDCA
- Executar as ações preventivas e corretivas
- Comunicar as ações de melhoria
- Assegurar-se de que as melhorias surtiram efeito.

Ao implementar melhorias e assegurar o efeito das mesmas, o ciclo garante a reciclagem de medidas de monitoramento que sejam eficazes e efetivas ao mesmo tempo, de modo a excluir a necessidade de um novo ciclo.

2.3.5 Análise de Riscos

Analisar os riscos de incidentes de segurança da informação é uma atividade essencial, da máxima importância para a gestão da segurança da informação. (CAMPOS, 2007, p.50).

Quanto a análise de riscos, Campos (2007), e Oliveira (2008) dizem em concordância, que analisando os riscos, torna-se possível identificar o grau de proteção que os ativos de informação de cada processo da organização precisam, permitindo assim, não apenas proporcionar a proteção em grau adequado para o negócio, mas principalmente usar de maneira inteligente os recursos da organização.

Para concluir, Campos (2007) mais uma vez enfatiza a importância da análise de riscos, ao declarar que é o coração do SGSI, pois sem essa análise seria impossível determinar

o conjunto adequado de medidas de segurança e garantir qualquer nível de sinergia nas ações tomadas.

2.3.5.1 Estratégia de avaliação de risco

A escolha da estratégia de avaliação de risco deve ser o primeiro passo da análise de risco. O objetivo é definir que resultados são esperados e, por conseguinte, que caminhos deverão ser percorridos. (CAMPOS, 2007, p.50).

Campos (2007) e Oliveira (2008) convergem ao expor os métodos utilizados para avaliação de riscos. Ambos autores falam que existem basicamente dois métodos de análise de risco: os **qualitativos** e os **quantitativos**, ambos melhor descritos no quadro 1.

Quadro 1 – Método de análises de risco

Quantitativo	**Qualitativo**
Resultados baseados em valores objetivos.	Resultados baseados em valores subjetivos.
Cálculos complexos.	Cálculos simples.
Valores financeiros são atribuídos ao risco.	Não há valoração do risco.
Grande tempo e esforço são necessários para atribuir as taxas de risco.	Menor trabalho para atribuir as taxas de risco
Facilita o cálculo de custo/benefício	Dificulta o cálculo de custo/benefício

Fonte: CAMPOS, 2007, p.51

Campos (2007) defende que ambos os métodos são práticos e interessantes e a escolha deve ser feita com base no perfil da organização.

Já Oliveira (2008) prefere se posicionar de modo a favorecer o método quantitativo, por embora ser mais complexo, trabalha com informações mais exatas, e por consequência, mais confiáveis, fazendo com que o método traga maior credibilidade ao resultado final.

Campos (2007) cita também, que para se avaliar os riscos, deve-se levar em conta as ameaças, quanto ao grau de exposição que apresentam para o ativo em questão.

Para definir os critérios de ameaças, Campos (2007) representa na tabela 1 a relação entre o **grau de exposição**, **valor nominal**, e **faixa percentual** da ameaça.

Tabela 1 - Grau de ameaça quanto a análise de riscos

Ameaça		
Grau de exposição	**Valor nominal**	**Faixe percentual**
Mínimo	1	01-20
Baixa	2	21-40
Média	3	41-60
Alta	4	61-80
Máxima	5	81-100

Fonte: CAMPOS, 2007, p.53

Entende-se por esta tabela, que quando o grau da ameaça é definido, pode-se determinar por consequência o quanto existe daquela ameaça, sem levar em consideração por enquanto, qual o ativo em questão. Ou seja, pode-se concluir baseando-se no exposto anteriormente, e baseando-se na tabela 2, que o grau da ameaça é propriedade única da própria ameaça.

Em frente e baseando-se nos conceitos bem explicados por Campos (2007), a próxima análise seria a de **vulnerabilidade** existentes nos ativos de informação, similarmente ao feito em relação às ameaças, como aparece na tabela 2

Tabela 2 - Grau de vulnerabilidade quanto a análise de riscos

Vulnerabilidade		
Deficiência de controles	**Valor nominal**	**Faixa percentual**
Mínima	1	01-20
Baixa	2	21-40
Média	3	41-60
Alta	4	61-80
Máxima	5	81-100

Fonte: CAMPOS, 2007, p.54

O critério que Campos (2007) utilizou para criar e avaliar esta tabela é simples, a vulnerabilidade é uma propriedade do ativo em relação a uma determinada ameaça, já que ativos diferentes, quando expostos à mesma ameaça, apresentarão vulnerabilidades em graus

diferentes. Além disso, alguns ativos já receberam algum tipo de proteção, que diminuiu sua vulnerabilidade, enquanto outros ainda não receberam proteção alguma, então utiliza-se esta tabela como proposta para calcular a vulnerabilidade de um ativo, em relação à ameaça.

Continuando rumo à conclusão de Campos (2007) sobre a estratégia de análise de riscos, ainda há uma última proposta para entrar na equação, sendo esta, a avaliação do **impacto,** ou seja, um prejuízo estimado para um incidente de segurança.

Apenas como exemplo, pode-se relacionar o grau do impacto à sua duração da interrupção que um determinado processo de negócio suporta, ou seja, que pode continuar operando sem causar grandes prejuízos.

A seguir a tabela 3 ilustra esta medida, seguindo ainda o conceito de Campos (2007).

Tabela 3 - Grau de impacto quanto a análise de riscos

Impacto		
Interrupção suportada	**Valor nominal**	**Faixa percentual**
Mínimo (mais de 1 mês)	1	01-20
Baixo (1 mês)	2	21-40
Médio (1 semana)	3	41-60
Alto (1 dia)	4	61-80
Máximo (1 hora)	5	81-100

Fonte: CAMPOS, 2007, p.54

Supondo uma organização qualquer, na qual os processos são fortemente baseados na troca de mensagens eletrônicas entre as áreas, supõe-se que a interrupção desse serviço não seria tolerada por mais que 1 dia, o que classificaria o impacto como alto.

Já o servidor de arquivos talvez seja usado com menos frequência ou intensidade, caso este em que a organização até poderia ficar alguns dias sem o serviço, assim então, talvez fosse possível classificar esse impacto como médio.

Conclui-se a partir disto então, que **ameaça**, **vulnerabilidade** e **impacto** andam juntos em relação a avaliação de riscos, sendo que na posse das 3 variáveis se torna possível a avaliação mais perto da realidade de um risco.

2.3.6 Política de Gestão de Segurança da Informação

Conceitualmente, como Oliveira (2008) resume, a política de segurança da informação é um documento que deve ser aprovado pela alta administração da organização, demonstrando comprometimento e apoio às determinações. Este documento, ou conjunto de documentos, deve ser publicado respeitando a necessidade de saber de cada área ou pessoa, e comunicado de forma adequada para todos aqueles que devem obedecê-la, sejam estes funcionários, parceiros, fornecedores ou terceiros.

Ainda seguindo este autor, este documento, ou conjunto de documentos, deve refletir, em alto nível, os objetivos do negócio, num nível intermediário os objetivos táticos e no nível mais baixo, os objetivos operacionais. E se os objetivos estiverem claros e alinhados, a aderência se dará de forma mais suave, uma vez que toda normatização ou obrigatoriedade sempre provoca resistência. Por isso a conscientização da organização a nível de pessoal é fator crítico para o sucesso da segurança da informação.

2.3.6.1 Importância de uma política de segurança

Todas as ações realizadas dentro de uma empresa contribuem, ou pelo menos devem contribuir, para os objetivos maiores dessa empresa. A política de segurança da informação deve, do mesmo modo, contribuir para esses objetivos, ou do contrário, será uma ferramenta sem valor para o negócio e, consequentemente, não será utilizada de fato. (CAMPOS, 2007, p. 130).

Campos (2007) ainda completa apresentando um fato interessante. Atualmente, política de segurança da informação é adotada em grande parte das organizações em todo o mundo, inclusive no Brasil. Mesmo aquelas organizações que ainda não têm uma política efetiva, reconhecem a necessidade de elaborar e implementar uma.

As normas NBR ISO/IEC 27001 e NBR ISO/IEC 27002, ambas específicas sobre segurança da informação, indicam que a política de segurança da informação é um controle essencial. (CAMPOS, 2007, p.131).

E diante de tudo isso, Campos (2007) conclui seu texto sobre o assunto, dizendo que como o principal objetivo da política de segurança da informação é estabelecer um padrão de comportamento que seja conhecido por todos, e que sirva como base para decisões da alta direção em assuntos relacionados à segurança, a política acaba em suma, proporcionando coerência nessas decisões e menos complexidade para se chegar a conclusões sobre assuntos diversos relacionados à segurança.

2.3.7 Implantação do SGSI

A implantação do SGSI em uma organização é estratégica para o seu negócio, pois, através dele, o gestor de segurança da informação tem condição de planejar, implantar, monitorar, analisar e executar ações corretivas em relação às brechas de segurança existentes na organização (LENTO, 2010, p.117).

O projeto e a implementação do SGSI são influenciados pelas necessidades dos negócios e objetivos, resultando em requisitos de segurança, processos adotados, tamanho e estrutura da organização. (LENTO, 2010, p.117).

2.3.7.1 Requisitos para a implantação do SGSI

De acordo com a norma NBR ISO/IEC 27001:2005 os requisitos para a implantação do SGSI estão distribuídos de acordo com a seção **2.3.4** deste trabalho, utilizando o ciclo PDCA.

2.3.8 Auditoria

O objetivo de uma auditoria é garantir a efetividade dos processos e ativos de uma determinada organização. A auditoria poderá dedicar-se a comprovar a eficácia, a eficiência ou a efetividade do SGSI. (CAMPOS, 2007, p.103).

Sabendo do objetivo da auditoria, pode-se então tentar explicar o conceito geral de auditoria, para isso, Lento (2010) cita Melo (200) ao falar que, a auditoria pode ser definida como uma atividade que engloba o exame das operações, processos, sistemas e responsabilidades gerenciais de uma determinada entidade, com o intuito de verificar a sua conformidade com certos objetivos e políticas institucionais, orçamentos, regras, normas ou padrões.

Lento (2010) cita Dias (2000) para expor que, uma outra forma de se vivenciar uma auditoria consiste em estabelecer e executar procedimentos para a coleta de dados gerados pela atividade de um sistema computacional. Estes dados então, podem ser utilizados na análise de segurança do sistema em questão, visando detectar quais falhas ocorreram, de modo que possam ser corrigidas e responder aos incidentes de segurança ocorridos.

Toda a auditoria é dividida em três fases de acordo com Lento (2010):

- **Planejamento –** identifica os instrumentos indispensáveis à sua realização
- **Execução –** reúne as evidências teoricamente confiáveis, relevantes e úteis para a realização dos objetivos da auditoria.
- **Relatório –** são apresentados os resultados, análises e conclusões por escrito.

Sabendo que toda a auditoria possui essas três fases, Campos (2007) exemplifica alguns tipos de auditoria.

2.3.8.1 Auditoria de primeira parte

Aquela realizada pela própria organização, conhecida também como auditoria interna. O objetivo desse tipo de auditoria é demonstrar as falhas no sistema de segurança da informação de modo que planos de ação para correção e melhoria possam ser elaborados e executados. É uma exigência da norma NBR ISO/IEC 27001 que a organização tenha um programa de auditoria de primeira parte estabelecido. (CAMPOS, 2007, p.103).

2.3.8.2 Auditoria de segunda parte

Realizada para avaliar se o SGSI está implementado de maneira correta, mas em outra organização, provavelmente validando auditorias internas já realizadas por aquela organização. Um exemplo típico é a auditoria por um cliente em seu fornecedor. (CAMPOS, 2007, p.103).

2.3.8.3 Auditoria de terceira parte

Segundo Oliveira (2008) é aquela auditoria realizada e reforçada por um órgão certificador na organização que deseja uma certificação NBR ISO/IEC 27001.

Completando essa afirmação, Campos (2007) diz que os resultados aparentes de receber tal certificação seriam principalmente o reconhecimento do mercado como uma empresa que respeita os princípios de segurança da informação, a certeza de que o sistema de segurança da informação da organização está de acordo com as normas e preceitos internacionais e, consequentemente, a possibilidade maior de que os processos, produtos e serviços da organização sejam melhores.

2.3.9 Aspectos de uma auditoria

O programa de uma auditoria deve ser planejado levando-se em consideração o estado e a importância dos processos e áreas a serem auditoradas, bem como os resultados das auditorias realizadas anteriormente. Na sequência, os aspectos que devem ser considerados (DIAS, 2000 *apud* LENTO, 2010).

2.3.9.1 Pesquisa das fontes de informação

É adquirida a maior quantidade de informação sobre a instituição a ser auditada e também do seu ambiente computacional, possibilitando estabelecer os aspectos iniciais do plano de auditoria. (LENTO, 2010, p.129).

Todo este conhecimento inicial possibilita à equipe de auditoria ter uma visão básica do grau de complexidade de todo o ambiente computacional (*hardware e software*) que irá encontrar, possibilitando que a mesma prepare-se tecnicamente e providencie os dispositivos necessários para a realização da tarefa (LENTO, 2010, p.129).

2.3.9.1.1 O que/onde coletar

Lyra (2008) neste quesito, expõe praticamente o mesmo de Campos (2007), Lento (2010) e Oliveira (2008) ao falar sobre coleta de dados de *hardware*, sistemas operacionais, SGBDs (Sistema Gerenciador de Banco de Dados) etc.

Lento (2010) completa dizendo que essas informações podem ser obtidas via entrevistas com os componentes das áreas, mas vale a pena ler os relatórios anteriores da auditoria, documentos que abordem os aspectos operacionais dos dispositivos de *software* e *hardware*, documentos sobre a segurança da empresa (política de segurança) etc.

2.3.9.2 Campo, âmbito e subáreas

Para toda essa seção, será utilizado o conteúdo apresentado por Lento (2010).

- **Campo** – o campo é composto por:
  - Objeto – Sistema de informação, área, setor, etc.
  - Período – Varia conforme a abrangência das tarefas a serem executadas.
  - Natureza – TI.
- **Âmbito –** avaliação da eficácia dos controles
- **Subáreas –** estão em concordância com o objeto a ser auditorado.

Entendendo do que se trata cada um dos conceitos, os recursos necessários e metodologias comuns ou úteis são apresentados a seguir.

2.3.9.3 Recursos necessários

Lyra (2008) e Lento (2010) representam brevemente os recursos como principalmente de origem humana, econômica e técnica, sendo a escolha da equipe, a previsão de gastos e quais os dispositivos de *hardware* e *software* serão utilizados.

2.3.9.4 Metodologias

Para concluir, a forma resumida proposta por Lento (2010) explica bem as metodologias existentes.

- Entrevistas

- Apresentação – realizada no início dos trabalhos para apresentação da equipe, cronograma de atividades, áreas a serem auditoradas, período etc.
- Coleta de dados – obtém-se dados sobre o sistema, ambiente computacional entre outros.
- Discussão – são apresentadas as deficiências encontradas e discutidas com seus respectivos responsáveis.
- Encerramento – é apresentado um resumo dos resultados da auditoria.

- Técnicas ou ferramentas de apoio
  - Análise de dados – os dados podem ser coletados e analisados com auxílio de *softwares*, por amostragem, arquivos, logs, etc.
  - Verificação de controles de sistemas – testa se os controles dos sistemas são realmente confiáveis.

O capítulo de revisão bibliográfica buscou contextualizar os principais conceitos de informação, segurança, gestão e auditoria de modo que ficasse claro todo o processo e boas práticas envolvidas na área de segurança como fundamento para a forense computacional.

Porém um perito forense não deve possuir somente conhecimentos referentes à segurança da informação, embora seja este seu carro chefe, um perito deve possuir conhecimentos avançados de programação, banco de dados, modelagem, documentação, redes de comunicação, estruturas de dados, algoritmos, análises performáticas, recuperação de arquivos, análises de documentos, etc.

Por esta extensa capacitação técnica, este trabalho necessita focar em um só método, exposto a seguir no capítulo 3.

3 MÉTODO

Segundo Candido e Saúde (2005) os métodos e procedimentos forense simplificam o processo de coleta, armazenamento e análise de evidências a partir de um incidente, minimizando o pânico e reações negativas em circunstâncias em que a perícia é conduzida sobre níveis elevados de estresse, evitando um possível comprometimento das evidências, além de contribuir para validar as evidências coletadas em um processo criminal, lembrando também de que a aplicação de tal método necessita de uma fase de planejamento para que seja corretamente aplicado, e que tenha resultados satisfatórios.

Madeira (2012) apresenta que a produção científica tem por base a aplicação do método científico, e com ele, procura-se criar uma interpretação precisa do mundo e de seus fenômenos, de tal forma que gostos pessoais, culturais e religiosos não interfiram para distorcer os resultados de uma pesquisa.

Madeira (2012) cita Wolfs (2007) para exemplificar as etapas do método científico, sendo estes:

- Observação e descrição de um fenômeno ou grupo de fenômenos;
- Formulação de uma hipótese que explica o fenômeno;
- Experimentação ou teste da hipótese;
- Interpretação dos resultados.

Para descrever as etapas do método científico não são absolutos, há de fato, outras maneiras de abordar uma investigação forense, de modo a levantar evidências e proteger um ativo de informação e evitar incidentes.

Então, em direção ao exemplificado por Candido e Saúde (2005) baseando-se nas informações disponibilizadas pelo *SANS Institute* quanto a metodologia de resposta a incidentes, que se mostra como uma “alternativa” ao método científico proposto por Madeira (2012) tem-se os seguintes passos de execução:

- **Preparação**: envolve o planejamento e definições de políticas para lidar com o incidente quando detectado.

- **Identificação**: caracterização da ameaça e seus efeitos nos sistemas afetados.
- **Contenção**: consiste em limitar o efeito do incidente de modo que atinja o menor número de sistemas possíveis.
- **Erradicação**: estágio no qual as consequências causadas pelo incidente são eliminadas ou reduzidas.
- **Recuperação**: retomada das atividades em andamento antes do incidente ocorrer. Também restauração de dados caso necessário.
- **Continuação**: medidas necessárias para evitar que a ocorrência do incidente seja repetida.

Há também, métodos para aplicação de uma perícia forense, exemplificados por Candido e Saúde (2005), sendo:

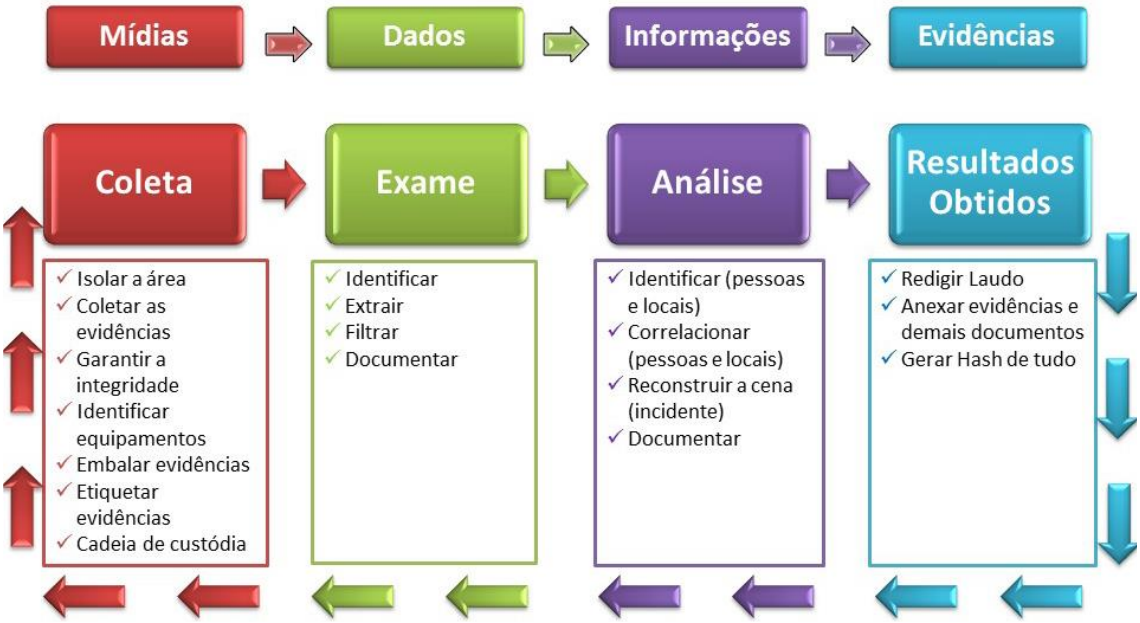
- Coleta de informações.
- Reconhecimento das evidências.
- Restauração, documentação e preservação das evidências encontradas.
- Correlação das evidências.
- Reconstrução dos eventos.

Para este capítulo, segue o modelo apresentado por Candido e Saúde (2005), com base no *SANS Institute*, visto que se assemelha com o ciclo PDCA, utilizando técnicas e processos descritos no ciclo, como visto no capítulo 2.

Além disso, este modelo serve de base para a elaboração da proposta deste trabalho para uma elaboração de investigação forense, principalmente nas fases iniciais e características de *loop*, o que faz com que o modelo possa ser reciclado sem perder a viabilidade.

Para melhor ilustrar o procedimento de investigação forense, a figura 6 mostra como é distribuído um esquema de investigação, esquema este que é seguido no decorrer deste trabalho.

Figura 6 - Ciclo de uma investigação forense



Fonte: Luis Vieira (CNASI 2001).

O esquema da figura ilustra como cada integrante da etapa de investigação é tratado, descrevendo as ações aplicadas sobre o mesmo de modo a seguir um “algoritmo” de atividades que possibilita a passagem para o próximo ativo, e à próxima etapa.

3.1 CARACTERIZAÇÃO DO TIPO DE PESQUISA

A principal característica de pesquisa do presente trabalho, se dá pela característica **teórica,** embora uma abordagem prática seja necessária para a validação da proposta deste trabalho. Segundo Aires (2003) a pesquisa teórica é toda pesquisa que analisa uma determinada teoria, não há experimentação, nem exploração. Apenas documenta-se os fatos obtidos, comparando com diversos autores.

Porém, o estudo de caso proposto como objetivo, por mais empírico que seja, sugere uma abordagem **experimental** já que todo o levantamento bibliográfico e teórico deste trabalho tem por finalidade a elaboração de uma solução que atenda os tipos de forense.

Fortemente presente neste trabalho, a pesquisa teórica no meio da forense computacional é de extrema importância de acordo com o pesquisado, é na teoria que mora o fundamento de toda prática, e neste trabalho, a abordagem teórica é fundamental pelo interesse do autor no assunto, e com o objetivo de coletar o maior número de informações e conhecimento sobre o mesmo afim de se construir uma carreira a partir deste.

A seguir, os cronogramas simplificado e detalhado (para o segundo semestre) sugeridos para este trabalho ilustra como a pesquisa será ministrada para os próximos capítulos, tendo em vista que serão estudados métodos e produções de resultados, de modo a compreender o funcionamento de uma aplicação de método investigativo forense, e como um relatório é apresentado a partir deste, além de se criar um modelo conceitual para planejamento e execução dos métodos estudados, a fim de validar a proposta deste trabalho.

Tabela 4 - Cronograma simplificado

	2013					2014					
	8	9	10	11	12	1	2	3	4	5	6
1 - Introdução	x										
2 - Fundamentação Teórica - Segurança e Gestão da Informação		x	x								
3 - Aplicação de métodos forense para ambientes corporativos			x	x							
4 - Análise da aplicação dos métodos forense para ambientes corporativos				x	x	x	x	x			
5 - Modelo conceitual e execução								x	x		
6 - Preparação do ambiente de validação									x	x	
6 - Compilação dos resultados obtidos										x	
7 - Conclusão											x
Defesa											x

Fonte: Autor (2013).

Tabela 5 - Cronograma detalhado - Março 2014

	Março			
Atividade	02 - 08	09 - 15	16 - 22	23 - 29
Cap. 4 - Finalização da pesquisa dos tipos de forense	x	x		
Cap. 4 - Levantamento de ferramentas para execução de análise forense (framework)	x	x	x	
Cap. 5 – Planejamento de execução do framework				x

Fonte: Autor (2014).

Tabela 6 - Cronograma detalhado - Abril 2014

	Abril			
Atividade	06 - 12	09 - 15	16 - 22	23 - 29
Cap. 5 - Preparação do ambiente para execução	x	x		
Cap. 5 - Planejamento do cenário de execução do framework		x	x	
Cap. 6 - Executar o plano de ação			x	x

Fonte: Autor (2014).

Tabela 7 - Cronograma detalhado - Maio 2014

	Maio			
Atividade	04 - 10	11 - 17	18 - 24	25 - 31
Cap. 6 - Levantamento dos resultados	x			
Cap. 6 - Análise dos resultados		x		
Cap. 6 - Produção dos relatórios		x		
Cap. 6 - Produção do laudo			x	
Cap. 7 - Conclusão				x

Fonte: Autor (2014).

Uma vez concebidos os cronogramas, pode-se perceber algumas limitações para a execução do planejado, exemplificados a seguir.

3.2 DELIMITAÇÕES DO PROBLEMA

A pesquisa e planejamento de execução deste trabalho revelaram alguns pontos chave de delimitações, que podem fazer com que o resultado final seja direta, ou indiretamente afetado. Tais delimitações podem ser constantes ou circunstanciais dependendo do caso em que a investigação foi requerida, sendo assim, tais delimitações são apresentadas a seguir:

- **Tempo**: O tempo disponibilizado para que o autor pudesse realizar uma investigação completa, levando em consideração todas as variáveis e desvios que uma investigação demanda não é viável para um trabalho completo, restringindo o autor a simular um estudo de caso em ambiente controlado a fim de demonstrar como uma investigação utilizando do modelo conceitual proposto iria decorrer, e quais resultados produzir.

- **Esforço:** A falta de tempo faz com que o autor não disponha da quantidade de esforço recomendada para se validar a proposta do trabalho, fazendo com que todos os resultados sejam novamente manipulados e simulados, se aplicando o máximo de conceitos e leis possíveis.

- **Capacitação técnica: Capacitação técnica:** Pelo fato de não existirem estudos de caso pouco complexos, toda forense requer um nível elevadíssimo de capacitação técnica do perito, devido a todas as particularidades, medidas preventivas, garantias de mantimento dos princípios de segurança, julgamento ao se analisar uma massa de dados, experiência para diferir uma suposição de uma informação, um dado de uma evidência, e saber também aplicar as leis corretamente em cima do que foi levantado, analisado e compilado.

Com base na figura 6 e todo o embasamento levantado no capítulo 2, o próximo passo deste trabalho no capítulo 4, foca nas práticas e métodos forense em geral, bem como suas variações, ferramentas necessárias para investigação e plataformas, de modo a se estabelecer uma base para a proposta deste trabalho no capítulo 5.

4 ANÁLISE DA APLICAÇÃO DE MÉTODOS FORENSE PARA AMBIENTES CORPORATIVOS.

Neste capítulo é realizado um estudo sobre as aplicações de métodos investigativos forense, bem como suas etapas e particularidades, de modo a reunir um conteúdo completo desde a preparação de uma investigação, até o estudo de ferramentas que possibilitem e viabilizem a investigação, e o bom trabalho do perito, dando origem a um novo modelo conceitual de investigação.

4.1 TIPOS DE FORENSE COMPUTACIONAL

A forense computacional apresenta-se por dois tipos principais, que possuem aplicações e utilidades únicas para determinado objetivo, mas que podem ser utilizadas em conjunto para que uma perícia seja bem efetuada, sendo elas **forense estática**, ou ***static forensic,*** e **forense dinâmica**, ou ***live forensic***. (MRDOVIC et al., 2011 – Tradução nossa).

As aplicações da forense podem ser derivadas em vários casos, e como Tavares (2010) exemplifica, a forense pode ser utilizada para:

- Fins legais, como casos de espionagem industrial, política, diplomática, etc. Casos como este também podem ser considerados *cyber* terrorismo, onde por influência política diplomática, são utilizadas técnicas de invasão para se obter vantagens ou influências políticas, ou socioeconômicas.
- Em ações disciplinares internas, como uso indevido de recursos da instituição/corporação/empresa. Comum de ocorrer em corporações grandes ou pequenas, muitas vezes os funcionários fazem mal uso dos recursos disponíveis, acessando *websites* indevidos, ou recorrendo a *e-mails* e softwares de mensagens instantâneas, podendo ser vítimas de engenharia social, e partilhar segredos da corporação que podem levar a danos muito maiores.

- Mais comumente em recorrência de uma ação ilegal intencionalmente ou não, em um alvo potencial, para investigação, tratamento de evidências, produção de laudos periciais, e validação de casos criminais.

No todo, Tavares (2010) esclarece que os tipos de forense são classificados pelo tipo de coleta de dados executada em cada um deles. Por exemplo, para a forense estática, tem-se a característica de análise e coleta de mídias de dados estáticos, como dispositivos de armazenamento, HDs, *Pendrives*, cartões de memória etc.

Na forense dinâmica são analisadas mídias de armazenamento volátil, como memória RAM.

4.2 FORENSE ESTÁTICA (*STATIC FORENSIC*)

Forense estática, também chamada de "forense tradicional", é o tipo de forense que trata de dados estáticos, ou seja, armazenados em discos rígidos, dados que não são perdidos ao se desligar o computador. (MRDOVIC et al., 2011 – Tradução nossa).

Mrdovic et al. (2011) explica que para que se aplique a forense estática uma cópia válida dos arquivos do sistema auditado precisa ser feita em primeiro lugar, para que seja possível aplicar as ferramentas de análise. Essas ferramentas focam em localizar arquivos e realizar uma pesquisa, ou busca em seu conteúdo diretamente, de modo que se torna possível identificar propriedades como datas de criação e modificação de arquivos, além de também ser possível recuperar dados como histórico de navegação, *logs* de *e-mails* e *softwares* instalados no sistema.

Mrdovic et al. (2011) ainda ressalva que para que se aplicar forense estática, o sistema precisa ser desligado, podendo executar essa tarefa procedendo com o algoritmo de desligamento de um sistema operacional, ou simplesmente "puxando o cabo de força", o que impede que prováveis *scripts* de remoção de evidências em caso de desligamento sejam executados, e em contrapartida pode fazer com que o disco fique em estado inconsistente, e dados em cache dessincronizados. Em ambos os casos de desligamento do sistema, o estado dinâmico é inevitavelmente perdido, exceto por dados paginados no disco.

Forense estática é geralmente aplicada em casos em que o incidente, ou suposto incidente, foi detectado com um espaço de tempo, ou **linha do tempo**, ou **perímetro temporal** relativamente grande, fazendo com que a investigação se baseie em *logs* e análises de discos em geral.

4.2.1 Análise estática

Como dito anteriormente, a análise forense estática lida com mídias de armazenamento, fontes de dados que não perdem as informações ao serem desligados, ou reiniciados, para isso, um conjunto de técnicas e ferramentas podem ser utilizadas para realizar uma análise estática.

Tavares (2010) explica a análise de dados estática em algumas etapas.

- **Cópia dos dados,** envolve a utilização de ferramentas adequadas para a duplicação dos dados.
- **Garantir e preservar a integridade,** caso a integridade não seja garantida, as evidências poderão ser invalidadas como provas perante a justiça. A garantia das evidências consiste na utilização de ferramentas que aplicam algum tipo de algoritmo *hash*.
- **Documentar** todos os objetos apreendidos na cena do crime, de modo que seja validada a análise e o alvo autenticado para produção posterior do laudo.

Como exemplo de documentação de evidências, Tavares (2010) traz um modelo de HD registrada como evidência no **Formulário de Cadeia de Custódia**[1], o que simplesmente registra o material apreendido em cena do crime para análise estática, ilustrado na figura 7, a documentação traz um código, uma descrição do equipamento apreendido, o fabricante, o modelo, número de série, e além do detalhamento da imagem dos dados criada a

[1] Formulário onde são registrados todos os dados provenientes da evidência coletada a fim de se controlar a entrada e saída de material coletado na investigação.

fim de se analisar propriamente os dados, sendo essas informações a data e hora da criação, quem foi o responsável por criar a imagem, o método utilizado para montagem da imagem, o nome da imagem, número de partes, e informações sobre a cadeia de custódia como, sequência, data e hora, origem, destino, e o motivo da apreensão.

Figura 7 - Formulário de cadeia de custódia

EVIDÊNCIA ELETRÔNICA

FORMULÁRIO DE CADEIA DE CUSTÓDIA

Caso Num.: 053203 Pag.: 01 De: 05

MÍDIA ELETRÔNICA/DETALHES EQUIPAMENTO

Item:	Descrição:	
00001	HD de Notebook com 80GB de capacidade	
Fabricante:	Modelo:	Num. de serie:
TOSHIBA	MK4026GAX	85MC7639T

DETALHES SOBRE A IMAGEM DOS DADOS

Data/Hora:	Criada por:	Método usado:	Nome da Imagem:	Partes:
20/5/2007 15:30	Paulo A. Neukamp	dcfldd	053203_01.dd	01
Drive:	HASH:			
Disco Completo	d243367072088feae98364977441d736			

CADEIA DE CUSTÓDIA

Seqüência:	Data/Hora:	Origem:	Destino	Motivo:
001	Data: 20/5/2007	Nome/Org.: Sigilo	Nome/Org.: Lab. Perí. Unisinos	Investigação sobre denuncia de Pedofilia
	Hora: 16:00	Assinatura:	Assinatura:	

Fonte: TAVARES, 2010

Neste caso, o HD (*Hard Drive*, ou disco rígido do computador, onde são armazenados todos os dados produzidos por usuários ou pelo sistema operacional) foi apreendido por suspeita de pedofilia, e será analisado estaticamente para levantamento, tratamento de evidências, e futura produção de laudo pericial, concretizando provas para juízo.

4.2.1.1 Cópia lógica (*backup*)

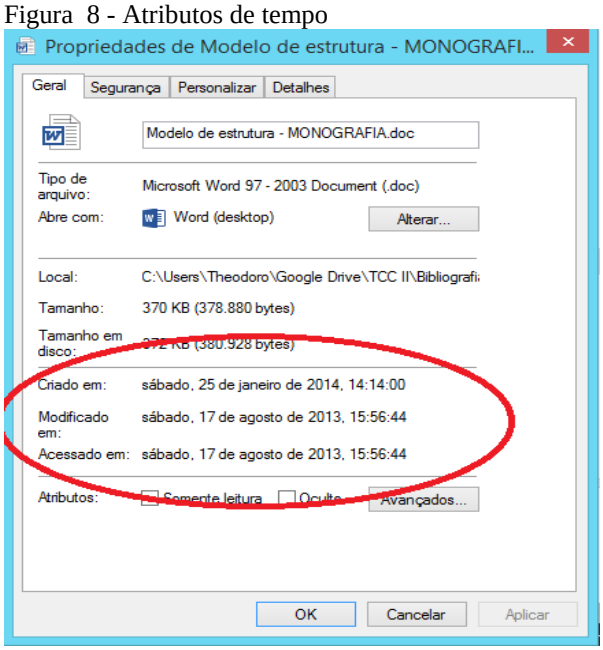
Segundo Tavares (2010) as cópias lógicas gravam o conteúdo dos diretórios e os arquivos de um volume lógico, porém não capturam outros dados como arquivos excluídos, ou fragmentos de dados armazenados nos espaços não utilizados, mas alocados por arquivos.

A imagem do disco, ou **cópia bit-a-bit** inclui os espaços livres e os espaços não utilizados. São algumas características da imagem de disco:

- Mais espaço de armazenamento consome mais tempo para copiar;
- Permitem a recuperação de arquivos excluídos e dados não alocados pelo sistema de arquivos.

Tavares (2010) em sua apresentação, ressalva também, que é importantíssimo manter 3 tributos de tempo relacionados aos arquivos, como exemplificados na figura 8.

Figura 8 - Atributos de tempo



Fonte: Autor, 2014

Esses dados são mantidos com cuidado para que a investigação não seja invalidada por conflito de dados de tempo, o que é vital para que a forense estática seja bem aplicada.

4.3 FORENSE DINÂMICA (*LIVE FORENSIC*)

Uma alternativa para a análise estática, ou mais especificamente uma abordagem complementar, é a forense dinâmica. Na forense dinâmica, são analisados os dados voláteis, dados que “morrem” ao desligar o sistema, que geralmente são armazenados na memória RAM. (MRDOVIC et al., 2011 – Tradução nossa).

4.3.1 Análise de memória volátil

Mrdovic et al. (2011) diz que uma prática comum na análise de memória volátil, é realizar uma cópia útil da memória para análise *offline* (forense estática). Isso possibilita que o perito possa construir o caso de investigação em um ambiente isolado que não cause nenhum tipo de obstrução à evidência. Além disso, uma vantagem da análise de memória, é a independência do sistema operacional da máquina supostamente comprometida.

A primeira ideia é utilizar um *hardware* pré-instalado que pode copiar memória para um dispositivo de armazenamento externo sem modificar seu conteúdo (MRDOVIC et al., 2011 – Tradução nossa).

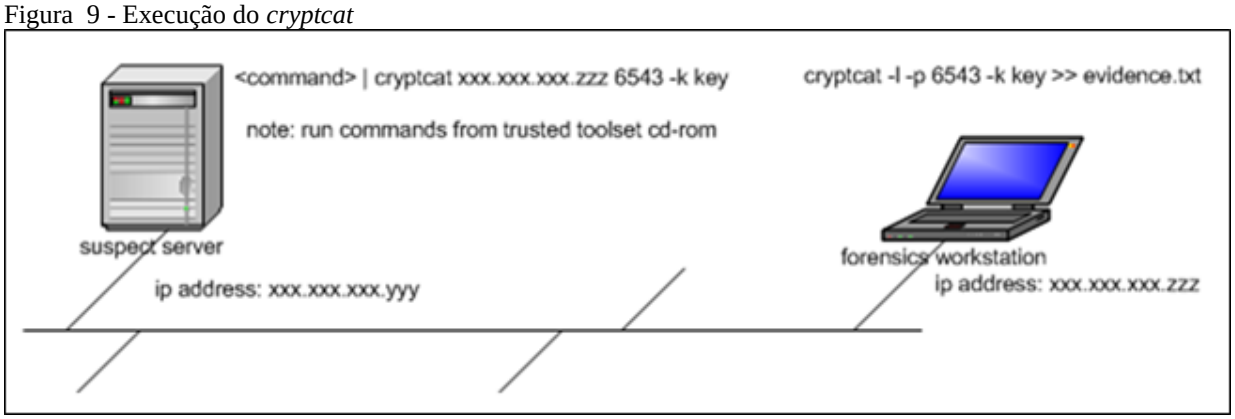
O principal benefício da análise de memória volátil é que ela requer um tempo mínimo ou nulo de hibernação do sistema, os dados são recuperados em tempo real, bastando que eles ainda estejam disponíveis na memória RAM para a descarga em arquivo, inutilizando possíveis teorias de alteração de informação que podem ser alegadas durante uma análise estática.

4.3.2 *Cryptcat* capturando memória volátil

A figura 9 mostra um exemplo muito utilizado de como capturar memória volátil. A área de trabalho utilizada para a realização da auditoria e aplicação de forense deve estar alocada na mesma LAN da máquina analisada.

Ferramenta do tipo *criptcat* podem ser usadas na área de trabalho para "ouvir" a porta do servidor.

Figura 9 - Execução do *cryptcat*



Fonte: GURJAR, 2013

Deve-se então, criar uma conexão aceitável e confiável e executar o seguinte comando:

criptcat <endereço IP> *6543 –k key*

E para copiar o resultado para a área de trabalho usa-se

criptcat –l –p 6543 –k key >> <nome do arquivo>

Este é apenas um exemplo de como cifrar informações de análise volátil para a área de trabalho para tráfego seguro, segundo Gurjar (2013).

4.4 PREPARAÇÃO

Tanto para Campos (2007) como para Candido e Saúde (2005), a etapa de preparação em uma estratégia de investigação forense consiste em etapas coincidentes com o ciclo PDCA.

Como no PDCA, a primeira medida a ser tomada é a definição de políticas a serem seguidas, e também ações a serem tomadas durante a perícia, em contrapartida aos eventos investigados, ou evidências coletadas durante a investigação. Esta etapa de definição se mostra essencial para que nenhum incidente passe sem um plano de ação, e para que a perícia seja bem aplicada.

Assim como no PDCA, após as definições das políticas e ações, deve-se estabelecer medidas preventivas para evitar o comprometimento do sistema computacional.

Definidas as políticas, ações e medidas preventivas, Campos (2007), Candido e Saúde (2005) definem também uma etapa de "pré-monitoramento", esta etapa consiste em um monitoramento no sistema computacional para que os incidentes possam ser detectados de modo que seja possível aplicar as medidas definidas.

Campos (2007) esclarece que, neste ponto já se encontram definidas as políticas, as medidas ou ações a serem tomadas em caso de detecção ou no caso da ocorrência de um incidente, por meio de monitoramento, ou pré-monitoramento, portanto, ainda não foram definidas ferramentas para executar a coleta e análise de evidências a partir de mecanismos de rede.

Segundo Candido e Saúde (2005) os mecanismos mais comuns e que podem fornecer informações valiosas para coleta e análise quando configurados corretamente são:

- *Firewalls/Sniffers/*Detectores de intrusão.
- Roteadores e *gateways* em geral.
- Servidores de *DNS*[2] e *Proxy*[3].
- Servidores de *backups*

---

[2] *DNS – Domain Name System* ou Sistema de Nomes de Domínio, é um sistema de gerenciamento de nomes hierárquico e distribuído visando resolver nomes de domínios em endereços de rede (IP). (Tradução nossa, fonte: <http://www.techterms.com/definition/nameserver>, acesso em 21/10/2013).

- Coletores de fluxos.

Avisos sobre alterações nos sistemas podem ser obtidos através do uso de ferramentas como o monitorador *Tripwire*[4], além disso, é recomendável também o uso de um *host* exclusivo para coletas de *logs*. Vale lembrar que *logs* locais podem ser facilmente removidos por um atacante com acesso administrativo, visto que uma vez acessado, o sistema disponibiliza os arquivos salvos para o atacante removê-los, ou alterá-los.

4.5 COLETA

Para Campos (2007), Carvalho (2005), Júnior e Saúde (2005), a coleta de evidências é feita principalmente com base nos dados obtidos a partir dos discos rígidos e demais mídias físicas.

Caso o sistema ainda esteja em funcionamento, pode-se recuperar evidências adicionais, com algumas medidas a serem tomadas baseando-se no documento produzido por Candido e Saúde (2005), sendo elas:

- É recomendável interromper a energia ao invés de desligar o sistema de modo habitual, fazendo isso se permite preservar o estado do sistema (*swap*, arquivos temporários, marcas de tempo (*timestamp*) nos arquivos etc.).
- Deve ser observado o tempo de vida de cada evidência encontrada, haja vista que toda mídia possui um tempo de vida útil.

Resumindo a coleta é a etapa onde todas as informações úteis e inúteis para a investigação são levantadas e quantificadas, para posteriormente serem filtradas em **análise.**

---

[3] *Proxy* – Um servidor *proxy* é um computador intermediário que fica entre o computador e a internet. Pode ser utilizado para registrar o uso da internet, e também bloquear acesso a determinados endereços da *Web*. *(*Fonte: <http://www.java.com/pt_BR/download/help/proxy_server.xml>, acesso em 21/10/2013).

[4] *Tripwire – Software "Open Source"* de segurança e integridade de dados, é uma ferramenta útil para monitorar mudanças específicas em arquivos em um, ou mais sistemas. (Tradução nossa, *software* disponível em: http://sourceforge.net/projects/tripwire/, acesso em 21/10/2013).

4.5.1 Dispositivos de armazenamento

Entende-se por dispositivos de armazenamento segundo o informado por Candido e Saúde (2005), por meios onde a informação possa ser gravada e recuperada respeitando os princípios da segurança de informação, a seguir alguns exemplos.

- Registradores e *cache*[5] que mesmo contendo pouca informação aproveitável são relevantes para coleta e análise por poderem conter informações importantes, mesmo que em quantidade menor.

- Memórias de periféricos, que contém normalmente informações não disponíveis na memória principal, como documentos enviados, imagens exibidas no monitor, etc.

- Memória RAM, onde se encontram informações sobre o sistema operacional e os processos em execução, podendo também conter senhas e informações em texto plano, que se encontram cifradas em disco.

- Discos Rígidos (HD) e mídias secundárias, oferecem a maior parte das informações usadas para extração de evidências, visto seu maior poder de armazenamento.

A coleta de mídias de armazenamento para análise se dá como um dos primeiros passos da investigação forense, como visto anteriormente neste capítulo, partindo das mídias, pode-se extrair informações vitais para a investigação, de modo que seja possível garantir a integridade, isolar equipamentos, etc.

---

[5] *Cache* é um dispositivo de acesso rápido, que guarda informações de acesso ou navegação, como imagens de um *website* ou termos pesquisados. O intuito do *cache* é facilitar e acelerar o acesso à informação de modo a facilitar a disponibilidade dos dados.

4.5.2 Alterações no sistema

As informações obtivas na coleta inicial podem não ser confiáveis uma vez que o sistema foi comprometido, violando os princípios da segurança e inviabilizando a continuidade da investigação.

Para que isso seja prevenido, recomenda-se utilizar *kit* forense para ambientes UNIX, que contém binários compilados estaticamente dos principais utilitários de sistema.

De acordo com Candido e Saúde (2005), tem-se como principais alvos de modificação de sistemas, os seguintes itens:

- *Shell*[6] este primeiro é de menor dificuldade de detecção, sendo então o primeiro alvo de mudança a ser investigado.
- Comandos do sistema podem ser investigados através do uso de *logs*, são mais difíceis de detectar do que as alterações de *shell* porém não podem deixar de serem investigados.
- Bibliotecas dinâmicas possuem um grau um pouco maior de dificuldade de detecção, segundo o documento disponibilizado *online* pela IBM, disponível em (http://www.ibm.com/developerworks/br/library/l-dynamic-libraries/), as bibliotecas dinâmicas são carregadas quando um aplicativo é carregado e a ligação ocorre no momento da execução, então a instância dinâmica torna a investigação mais difícil, requerendo um grau maior de foco a esse alvo.
- *Drivers* de dispositivos são alterados constantemente, sendo frequentemente atualizados, ou substituídos, sendo assim, pode ser realmente mais difícil detectar esta mudança de modo satisfatório, ou de modo a isolar um problema.

---

[6] *Shell* é um módulo que atua como interface usuário - sistema operacional, possuindo diversos comandos internos que permitem ao usuário solicitar serviços do sistema operacional. (Fonte: http://www.vivaolinux.com.br/artigo/Uma-introducao-ao-shell-(parte-1)/, acesso em: 21/10/2013).

- *Kernel* ou núcleo do sistema operacional, se mostra o mais complicado de se detectar modificações, por sua complexidade natural de exercer o controle do SO.

Alterações no sistema quando detectadas podem interferir no processo de investigação de modo a desacelerar ou impossibilitar uma análise completa, análise esta que se apresenta como próxima etapa.

4.6 ANÁLISE

Campos (2007), Carvalho (2005), Candido e Saúde (2005) salientam que a análise sempre deve ser efetuada sobre uma cópia das mídias originais, sem deixar de se preocupar com a proteção e segurança das mesmas.

Sendo assim, observa-se que a cópia deve ser *bit* a *bit*[7] com o intuito de preservar arquivos removidos, e outras informações que possam estar contidas na mídia original.

Além disso, as informações que são coletadas de suas mídias originasis, devem ser autenticadas através de assinaturas criptográficas.

Outro ponto observado pelos autores, é que a análise de dados brutos em disco e em memória é excessivamente lenta, e o uso de ferramentas para recuperação de arquivos e *dump*[8] de processos pode agilizar a análise.

Um ambiente de teste deve ser preparado de modo a auxiliar não somente a velocidade da análise, mas também a qualidade do trabalho realizado. Importante destacar, que o *hardware* utilizado para realizar as análises necessárias, deve ser preferencialmente similar, ou se possível idêntico, ao *hardware* original do ambiente original.

Por fim, todos os processos de análise com todas suas etapas devem ser devidamente documentados.

---

[7] Cópia *bit* a *bit* é uma cópia inteira e exata do estado do disco rígido alvo, aqui é produzido um arquivo que representa a área de trabalho e análise da investigação.

[8] *Dump* é um programa utilizado para realizar *backups* em um sistema de arquivos, operando em blocos, usualmente “abaixo” das camadas de arquivos do sistema operacional, ou sistema de arquivos. (Tradução nossa, fonte: http://www.coredumps.de/doc/dump/zwicky/testdump.doc.html, acesso em 21/10/2013).

4.7 RECONSTRUÇÃO DE EVENTOS

A reconstrução de eventos baseia-se em aspectos simples dentro de uma análise, nesta etapa, Candido e Saúde (2005) listam algumas atividades a serem executadas:

- Correlacionamento de *logs*.
- Análise do tráfego da rede (*logs* de roteadores, *firewalls*, diagnósticos de softwares, etc).
- Histórico do *shell* quando disponível,
- *MAC*[9] *Times.*
- Recuperação de arquivos apagados ou análise do *dump* do disco.
- Análise de artefatos encontrados no sistema.

Reconstruir eventos é bolar uma plataforma, ou um campo de ação o mais próximo do real possível, para que se possa aplicar ferramentas de monitoramento, análise, coleta e tratamento de acordo com o cada caso.

4.8 FERRAMENTAS PARA MONITORAMENTO

A seguir uma lista de utilitários para monitoramento e análise, utilizados por muitos peritos e populares da área.

- Monitorando mudanças no sistema de arquivos:
    - *Tripwire* (disponível em: http://www.tripwire.com).
    - *Aide* (disponível em: http://www.cs.tut.fi/~rammer/aide.html).

---

[9] *MAC* é um endereço físico associado à interface de comunicação, que conecta um dispositivo à rede.

- Centralizando os *logs*
    - *Syslog-ng* (disponível em: http://www.balabit.hu/en/downloads/syslog-ng).
- Identificação de *rootkit*[10]*s*.
    - *Chkrootkit* (disponível em: http://www.chkrootkit.org).
- Registro de conexões
    - *TCPwrapper*[11]

Monitoramento se enquadra como contramedida perante uma ação externa ou interna, sendo esta ação investigada ou potencialmente maliciosa.

4.8.1 Coletando dados brutos

Têm-se como definição comum para dados brutos os dados que foram recuperados ou pesquisados da mesma maneira que foram armazenados.

Na forense computacional, Carvalho (2005), Candido e Saúde (2005) ilustram via linhas de comando executáveis como executar cada método de coleta de dados brutos, mostrados a seguir (comandos aplicáveis a base Unix).

- *Dump* da memória pode ser executado via as seguintes linhas de comando:
    - *dd if /dev/mem of <destino>*
    - *dd if /dev/kmem of <destino>*
    - *dd if /dev/rswap of <destino>*
- *Dump* nos discos
    - *dd if <dispositivo> of <destino>*

---

[10] *Rootkit* - kit que permite controlar de maneira absoluta o computador. A principal característica deste tipo de arquivo é esconder-se nos sistemas operacionais para que esses usuários mal intencionados possam fazer o que quiserem quando bem entenderem. fonte: http://www.tecmundo.com.br/antivirus/2174-o-que-e-rootkit-.htm#ixzz2wHDknS3p

- Obtendo dados da memória da placa de vídeo
  - *xwd –display :0 –root > screen.xwd*
  - *xwud –in screen.xwd*
- Transferindo informações coletadas através do *Netcat*[12]
  - Servidor: *nc –p <porta> -l > <saída>*
  - Cliente: *<comando_do_sistema> | nc –w 3 to <porta>*

Coletar dados brutos fornece ao perito uma massa de dados ainda não filtrada, porém coerente perante os parâmetros determinados para tal coleta, como perímetro temporal, por exemplo.

4.8.2 Estado da rede

Para analisar e levantar informações gerais sobre o estado da rede são necessários alguns comandos simples de serem lembrados e executados, como apresentam Carvalho (2005), Candido e Saúde (2005).

- Para analisar as configurações da rede:
  - *ifconfig, iwconfig*
  - *route*
  - *arp*
  - *netstat –tupan, lsof –i*
- Para coletar informações de tráfego
  - *tcpdump –l –n –e –x –vv –s 1500*
  - e*thereal*

---

[11] Segundo Venema (2000) *TCPwrapper* é uma aplicação de acesso de controle baseada em *host* utilizada para bloquear e/ou controlar o acesso a servidores. Funciona basicamente em sistemas operacionais com base em UNIX. (Tradução nossa).

[12] *Netcat* é uma ferramenta de rede, disponível para sistemas operacionais Unix, Linux, Microsoft Windows e Macintosh que permite, através de comandos e com sintaxe muito sensível, abrir portas TCP/UDP e HOST. (Site oficial: http://netcat.sourceforge.net/).

4.8.3 Coletando informações sobre o estado do sistema

Coletadas as informações de rede, tráfego e mídias, o próximo passo é coletar informações sobre o estado do sistema em si, para isso, Carvalho (2005) disponibiliza alguns comandos que auxiliam esse propósito.

- Coletando *logins* de usuários
  - Verificar quem está logado atualmente: *w, who*
  - Últimos logins efetuados: *last*
  - Último acesso de cada usuário: *lastlog*
- Coletando informações sobre os processos do SO
  - Processos que atualmente estão em execução: *ps auxeww, ps ealf, ls /proc/*
  - Últimos comandos executados: *lastcomm*
  - Arquivos abertos: *lsof*
- Kernel e módulos:
  - Configurações gerais: *uname –a*
  - Módulos carregados: *lsmod, cat /proc/modules*
  - Módulos ocultos: *kstat –M.*

4.8.4 Informações do sistema de arquivos

Resta então, coletar informações sobre o sistema de arquivos, e para tal, Candido e Saúde (2005) listam alguns comandos complementares úteis para tal fim.

- Para recuperar informações do *MAC Time*:
  - Horário de último acesso: *ls –altu*
  - Tempo de alteração: *ls –alt*
  - Tempo de mudança nas permissões: *ls –altc*

- Propriedade de um arquivo específico:
  - *stat <arquivo>*
- Registro de todos os arquivos presentes no sistema:
  - *find / -type f –print0 | xargs -0 md5sum > <saida>*

4.8.5 Informações do alvo

Segundo informações de Giavaroto e Santos (2013), na etapa de coleta das informações do alvo, nada pode ser descartado. Todas as informações relacionadas ao segmento da empresa, desde servidores e *firewalls*, até os costumes dos funcionários da empresa, amigos, pessoas que possuem alguma relação com a empresa, empresas terceirizadas, *e-mails*, telefone, e quaisquer tipos de informações que chegam ao lixo.

Ainda seguindo a linha lógica aplicada por Giavaroto e Santos (2013), pode-se ainda ser aplicada engenharia social, onde, como citado no capítulo 2, utiliza-se de falhas humanas e até mesmo da "ingenuidade" dos colaboradores para se obter informações valiosas, sem que os mesmos saibam que estão contribuindo para um ataque, e causando uma ameaça para a empresa.

Giavaroto e Santos (2013) citam as informações do alvo como a primeira de 5 etapas características no procedimento da construção de um ataque *black hat*, o que para um auditor, também significam 5 etapas características para que seja possível um resultado satisfatório da auditoria aplicada, visto que um bom auditor deve pensar como um atacante, a fim de ter conhecimento o suficiente para receber um problema, e saber como proceder.

A seguir uma descrição das 4 etapas restantes de um ataque *black hat* para auditoria divididos em tópicos.

4.8.6 Varreduras de sistema

Giavaroto e Santos (2013) ressaltam que, uma vez coletadas as informações do alvo, pode-se utilizar a ferramenta de *pentest*[13] adequada para explorar o objetivo da auditoria. Nesta etapa, serão considerados *hardwares*, servidores, *firewalls*, tipos de serviços e portas específicas.

"A verificação de IDS/IPS[14] presente na rede deve ser analisada com um critério maior, a fim de aplicar mecanismos engenhosos relacionados à dificuldade imposta pelo sistema-alvo" (GIAVAROTO; SANTOS, 2013, p.22).

4.8.7 Ganhando acesso ao sistema

"Nesta fase, o sistema é violado, devido à descoberta de vulnerabilidade, a invasão é consolidada e, através dela, podemos explorar as camas internas do sistema, a fim de descobrir outros meios, pelos quais possa potencializar nosso ataque. " (GIAVAROTO; SANTOS, 2013, p.22).

Ainda seguindo o exposto por Giavaroto e Santos (2013), Podem-se verificar as estruturas de diretórios, políticas, senhas, e toda informação em contexto *root*[15], além da possibilidade da ampliação do reconhecimento do sistema conforme a necessidade de coleta de informações novas e relevantes para a auditoria. Importante destacar ainda, que uma análise geral do sistema ou mapeamento geral e detalhado será caracterizada pela personalidade de cada indivíduo invasor, e a vivência e experiência do invasor permitem diferentes ações não específicas, o que pode levar a várias situações inesperadas.

---

[13] *Penetration test* – "...Trata-se de um método para testar e descobrir vulnerabilidades em uma rede ou sistemas operacionais, onde são analisadas e exploradas todas as possibilidades de vulnerabilidade. " (GIAVAROTO; SANTOS, 2013, p19).

[14] *IDS/IPS – Intrusion Detection System/Intrusion Prevention System*- Sistema de detecção de intrusão/Sistema de prevenção de intrusão.

[15] *Root* – Ambiente de administração do Sistema Operacional, usuário com permissões de leitura e escrita em todo o sistema de arquivos.

4.8.8 Mantendo o acesso no sistema

Uma vez dentro do sistema com acesso *root*, utilizando de um conjunto de técnicas, é possível verificar a instalação de *rootkits*, *backdoor*, etc.

"... bem como outros métodos que possam contribuir com as facilidades que necessitamos, como portas abertas e organização de arquivos e estruturas ao nosso favor verificando se o sistema realmente está apto a dificultar determinadas ações." (GIAVAROTO; SANTOS, 2013, p.22).

Prosseguindo com este cenário, Giavaroto e Santos (2013), é necessária a inserção de uma estrutura maliciosa, com a qual possa contribuir a ratificação de um *pentest* real. Desta forma, tem-se uma situação consolidada, que contribuirá com a aplicação de mecanismos de defesas e bloqueios inerentes ao sistema trabalhado. Então, deve-se compreender que tais invasões ao sistema nem sempre influenciam na ruptura do sistema operacional e em arquivos, pois na maioria das intrusões consolidadas, os invasores estão atrás de informações que poderão contribuir quase sempre em ações que possibilitem lucros ou situações relacionadas ao crime.

Compreendendo as etapas decorrentes de um ataque, pode-se planejar um ciclo de investigação para que o auditor possa coletar informações, planejar e executar um plano de ação.

4.9 FERRAMENTAS PARA ANÁLISE

Esta seção do trabalho trata do início da aplicação prática da forense computacional, sob uma auditoria em rede utilizando métodos e ferramentas/plataformas para coleta e tratamento de informações.

4.9.1 Sistema Operacional - SO

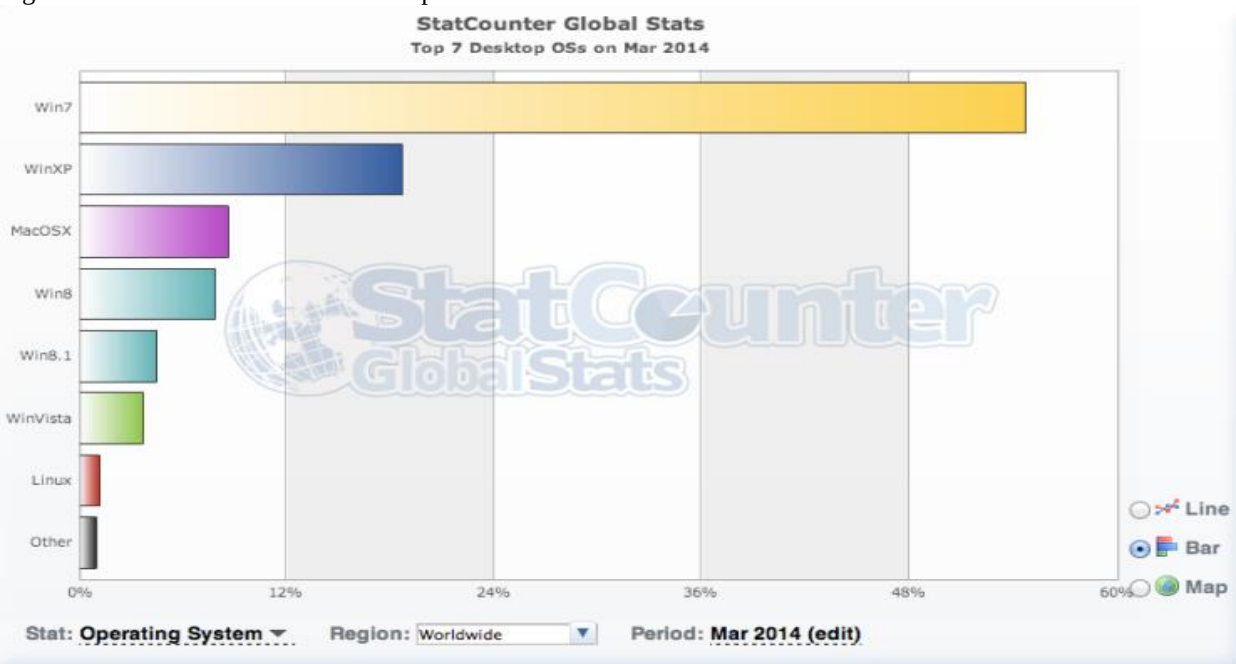
O sistema operacional neste trabalho, é apontado como plataforma para execução de ferramentas de coleta, análise e tratamento de informações.

Devido à grande quantidade de ferramentas disponíveis, e dos vários tipos de execução, este trabalho terá seu foco prático em duas plataformas, visando a praticidade e o desempenho esperado de cada tipo de ferramenta.

4.9.1.1 *Microsoft™ Windows®* 8.1

Windows, conforme ilustrado na figura 10, é o sistema operacional mais utilizado no mundo.

Figura 10 - *Status* de uso de sistemas operacionais no mundo em 2014



Fonte: <http://techcrunch.com/2014/04/02/discontinued-windowsxp-still-no-2-desktop-os-after-windows7-windows-8-lagging-far-behind/?utm_campaign=fb&ncid=fb>

Assim sendo, a utilização desta plataforma em uma investigação é quase que mandatória para um perito, visto que 9 (nove) entre 10 (dez) máquinas presentes em um

ambiente corporativo contratante com certeza utilizarão *Windows*. Além disso, esta plataforma possui fácil acesso às ferramentas nativas que podem reduzir o tempo da investigação e o retrabalho, ainda fornecendo ações e contramedidas.

4.9.1.1.1 NESSUS

Segundo o Luchi (2013), o NESSUS é uma das ferramentas mais conhecidas e completas para descoberta de vulnerabilidades, é gratuito apenas para uso doméstico, e pode ser encontrado no site **www.nessus.org**. Contando com centenas de plugins para descoberta de vulnerabilidades nos sistemas e serviços, é indispensável quando estiver em busca de vulnerabilidades.

A seguir, a figura 10 ilustra o NESSUS em execução, e em modo de exibição de vulnerabilidades, analisando a figura, pode-se observar que cada vulnerabilidade pode se enquadrar em 3 escalas de acordo com sua gravidade, além de ilustrar quais vulnerabilidades são pertencentes a qual categoria, ou “família”.

Figura 11 - NESSUS em execução

Fonte: LUCHI, 2013.

De posse desses dados, podem-se pesquisar as vulnerabilidades individualmente para melhor adequar a segurança do sistema.

Segundo dados do site **www.nessus.org**, a ferramenta possui mais de 60.000 (Sessenta mil) ferramentas e plug-ins, além de uma equipe técnica exclusiva para suporte, e seus *deploys* são simplificados pelo sistema *Amazon Web Services Cloud*.

4.9.1.1.2 RETINA

Segundo Stephenson (2010), o RETINA *Network Security Scanner* (*Scanner* de segurança de rede) desenvolvido e distribuído pela *eEye Digital Security*, disponibiliza gestão de vulnerabilidades multi-plataforma.

Este produto pode identificar tanto vulnerabilidades conhecidas, como vulnerabilidades ainda não descobertas ou exploradas, que podem vir a ser aproveitadas via ataque de tipo *zero-day*[16].

Ainda seguindo o exposto por Stephenson (2010), este *software* é pago, e sua instalação pode ser modular, completa, ou pode-se instalar componentes separados de maneira *standalone* (independente), sendo assim, o RETINA se mostra um *software* versátil e por consequência adaptável à necessidade do usuário final.

Stephenson (2010) ainda explica, que essa solução analisa pedaços específicos dos sistemas operacionais, aplicações e políticas, o que o possibilita a localização precisa de componentes vulneráveis e aponta ainda como um *hacker* pode explorá-la de modo a causar qualquer tipo de dano.

A seguir, a figura 12 mostra uma tela de relatório básica onde exibe os *scans* anteriores, e por data, qual o tipo de *scan* foi efetuado, com informações do sistema de arquivos, data de execução e tipos de vulnerabilidades escaneadas, além de qual *host* foi escaneado e como foi escaneado.

Ataque *zero-day* por sua natureza de ser um "ataque surpresa" muitas vezes deixa vestígios que possibilitam futuras contramedidas para ataques que possuírem as mesmas

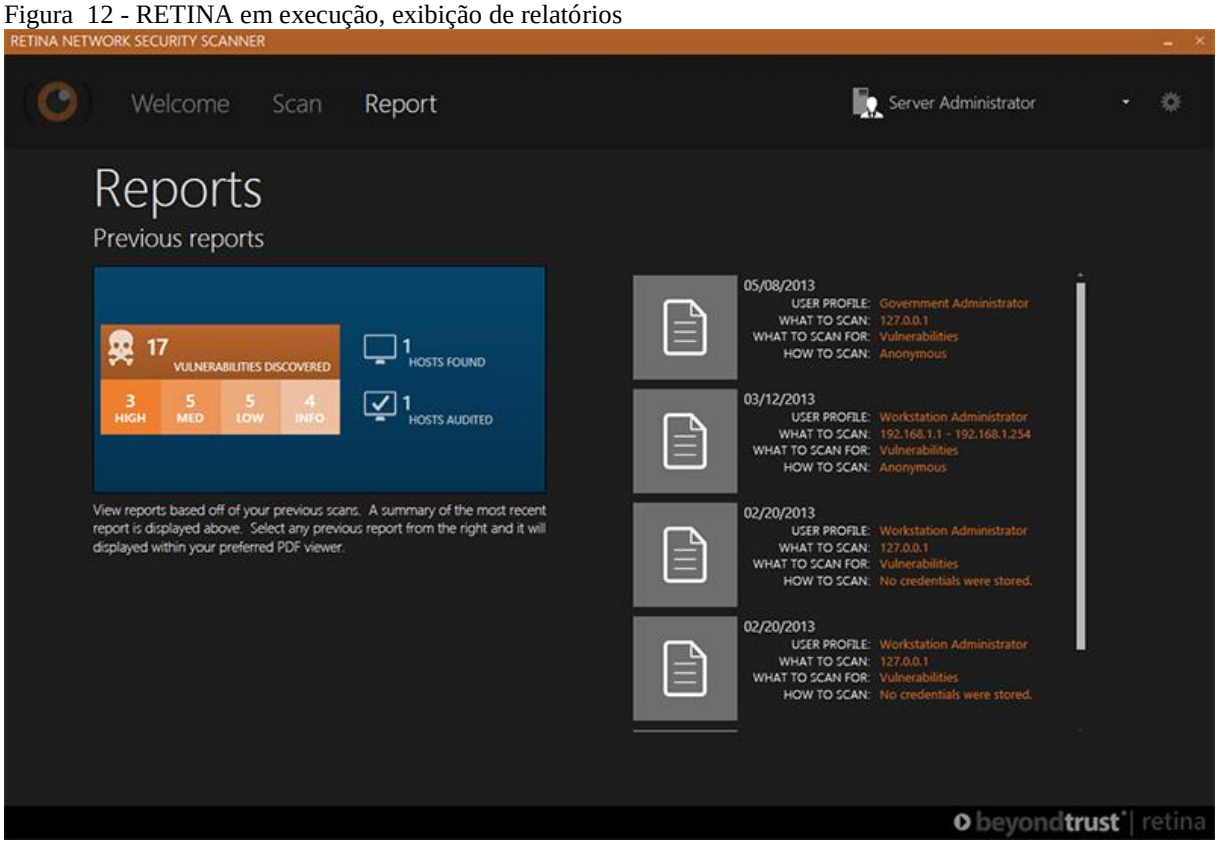
---

[16] Ataques de tipo *zero-day* são ataques que se aproveitam de uma vulnerabilidade imediatamente após sua descoberta, ou seja, se passaram "zero dias" entre a descoberta e o ataque. A ameaça desse tipo de ataque é enorme, visto que não se pode defender de um ataque desconhecido, só é possível lidar com as consequências, segundo Rouse (2010).

características, e para isso, o RETINA pode ajudar a facilitar a detecção de tais vestígios e possibilitar que o investigador defina mais rapidamente as contramedidas necessárias.

Por isso, de acordo com o pesquisado, o RETINA pode se encaixar tanto no planejamento de uma ação (*PLAN*, de acordo com o PDCA), como na revisão de ações (*CHECK*).

Figura 12 - RETINA em execução, exibição de relatórios



Fonte: < http://www.beyondtrust.com/Products/RetinaNetworkSecurityScanner/> Acesso em 30 mar 2014.

Além do RETINA, ferramentas como o *WIRESHARK* também podem integrar uma investigação em base *WINDOWS*, como exemplificado no próximo tópico.

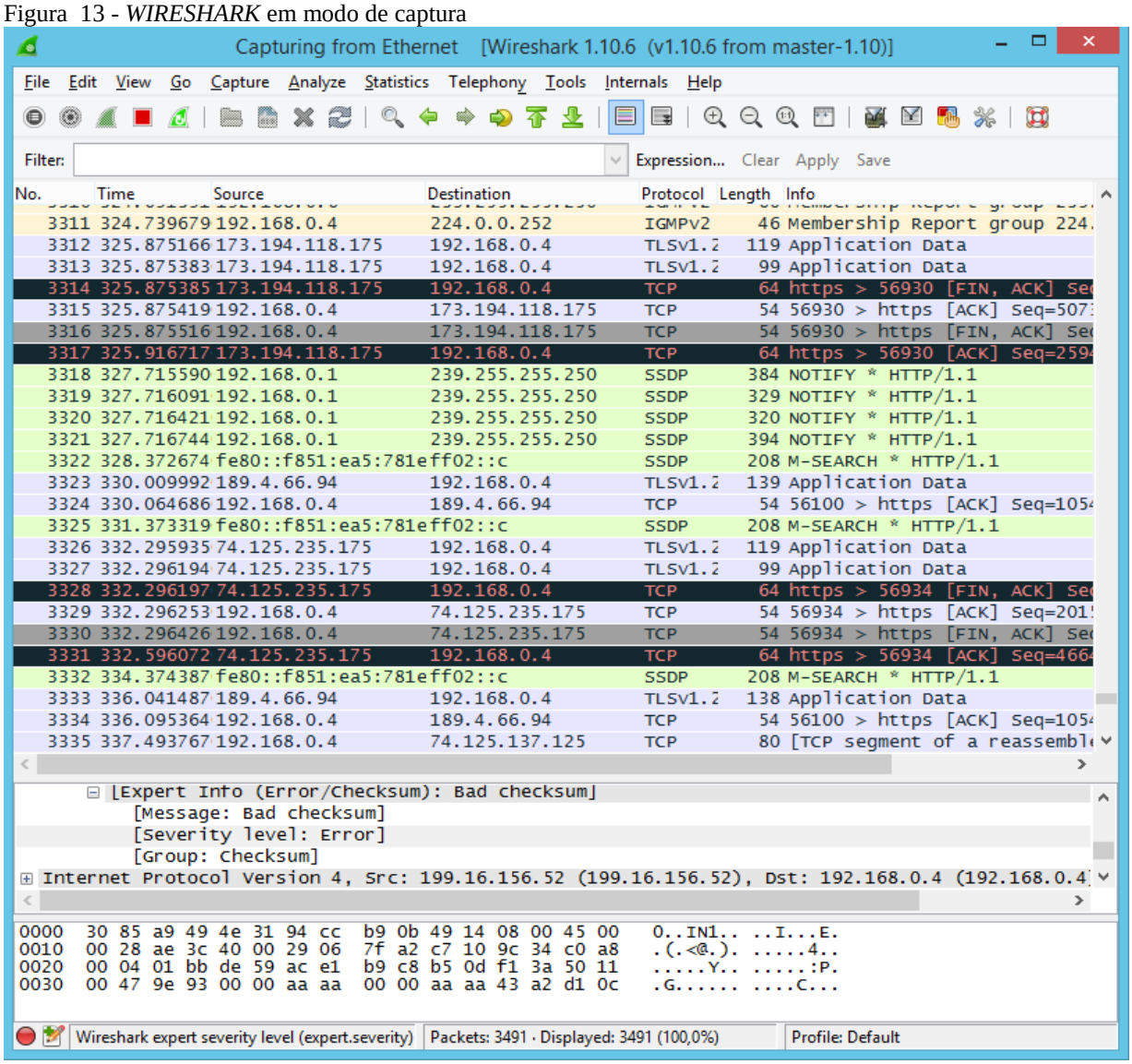
4.9.1.1.3 WIRESHARK

O *WIRESHARK*, segundo o *website* do próprio sistema (**www.wireshark.org**), é a ferramenta analista de protocolo de rede mais utilizada no mundo, ele permite que seja

visualizado o que está acontecendo em uma rede de computadores a níveis microscópicos, e por isso, acaba sendo a ferramenta padrão em qualquer *kit* de profissionais de segurança.

A seguir, a figura 13 ilustra a execução do *wireshark*.

Figura 13 - *WIRESHARK* em modo de captura



Fonte: Autor, 2014

Neste modo, a ferramenta apresenta todos os dados de tráfego necessários para coleta de informação, tais como origem, destino, tempo de resposta, protocolo que está sendo utilizado qual o *length* ou seja, qual o tamanho do pacote, e os demais detalhes relevantes ficam sobre responsabilidade da coluna “info”.

4.9.1.2 Linux Kali 1.0.6 via Oracle™ VirtualBox

Segundo a documentação disponibilizada no *website* da distribuição, Kali, é uma reconstrução completa do *BackTrack* Linux, e como seu predecessor, o Kali também é conhecido como o "canivete suíço dos profissionais de segurança de informação", que adere totalmente aos padrões de desenvolvimento do *Debian*. Uma infraestrutura completamente nova foi montada, todas as ferramentas (mais de 300) foram revistas e empacotadas, e foi adotado o Git [17]como controle de versões.

Ainda seguindo a documentação disponibilizada no *website* da distribuição, o Kali dispõe das seguintes *features* que devem ser levadas em conta e utilizadas neste trabalho:

- Mais de 300 ferramentas de testes de intrusão, mesmo depois de rever e corrigir ou descartar ferramentas do antigo *BackTrack*, o Kali ainda possui um número considerável de ferramentas úteis para um profissional de segurança.

- Complacente com o padrão FHS, o Kali foi desenvolvido para aderir ao Padrão Hierárquico do Sistema de Arquivos (ou FHS da sigla em inglês), permitindo que todos os usuários Linux facilmente localizem arquivos binários, de apoio, bibliotecas, etc.

Diferentemente do *Windows* o trabalho feito no Kali é quase completamente em modo console, ou seja, baseado em *prompt* de comando, sendo poucas as ferramentas que de fato oferecem interface gráfica, tornando o processo de coleta de informação e análise mais rápido, por possibilitar a execução de somente os comandos relevantes referentes a auditoria. Dentre as ferramentas presentes no Kali, este trabalho irá utilizar um número limitado de ferramentas como um *toolkit*, visto o tempo, e a complexidade do estudo que requer hosts ativos e confiáveis para execução.

---

[17] Git é um controlador de versões *online, open source*, que possibilita que os usuários possam controlar versões de arquivos, possibilitando a reversão de alterações, cópias de revisão, e todas as facilidades que um controlador deste tipo pode trazer para um ambiente corporativo, ou doméstico (apesar de não ser comumente utilizado domesticamente). Disponível em: < http://git-scm.com > Acesso em 30 mar 2014.

As principais ferramentas integrantes do Kali que possibilitam a realização de levantamento de informações são:

- HPING3 – Giavaroto e Santos (2013) descreve o HPING3 como uma ferramenta poderosa, capaz de detectar *hosts*, regras de firewall e também realizar varreduras de portas.

- FIERCE DNS – *fierce* é traduzido para o português como feroz, que é a principal característica dessa ferramenta, que pode trazer informações como o processador do computador *host*, o processador da máquina do servidor, bem como detalhes do sistema operacional, como ilustrado na obra de Giavaroto e Santos (2013).

- NMAP e NETCAT – Giavaroto e Santos (2013) descreve as duas ferramentas como similares, sendo úteis principalmente na fase *fingerprint*, onde possibilitam a varredura de portas, e obtenção da versão do sistema operacional, e dos aplicativos ativos no *host*.

- Netbios com Nbtscan – Presentes na obra de Giavaroto e Santos (2013) como ferramentas de enumeração, permitindo a recuperação do MAC e nome da máquina.

- AMAP – Definida na documentação de Giavaroto e Santos (2013) como uma grande alternativa para realizar enumeração, o AMAP tenta identificar aplicações ainda que estejam sendo executadas em uma porta diferente da usual, exemplo um servidor apache rodando na porta 4001 ao invés da porta 80.

- Metasploit – Giavaroto e Santos (2013) descrevem o metasploit como uma das ferramentas mais utilizadas pelos profissionais de segurança, e trabalha com *exploits*[18], *payloads*[19], *e shellcode*[20].

---

[18] Código de programação escrito com o intuito de explorar uma determinada vulnerabilidade.

- Medusa – Utilizado para ataques remotos obtendo senha através de força bruta, segundo Giavaroto e Santos (2013).

- *Autopsy Forensic Browser*- Segundo o próprio *website* da ferramenta (http://www.sleuthkit.org/autopsy), é uma plataforma digital de interface gráfica, que possibilita a execução de ferramentas e metodologias forense. Pode ser utilizada para polícia, exército, e investigadores em corporações.

Uma vez reunidas essas informações, ferramentas e plataformas úteis para se realizar uma investigação forense, e o que elas buscam e tratam, inicia-se o planejamento da prática e validação da proposta deste trabalho.

---

[19] É a carga do código aplicada ao sistema alvo, onde é possível a abertura de comunicação entre o atacante e o alvo, exemplo a obtenção de um *prompt* de comando.

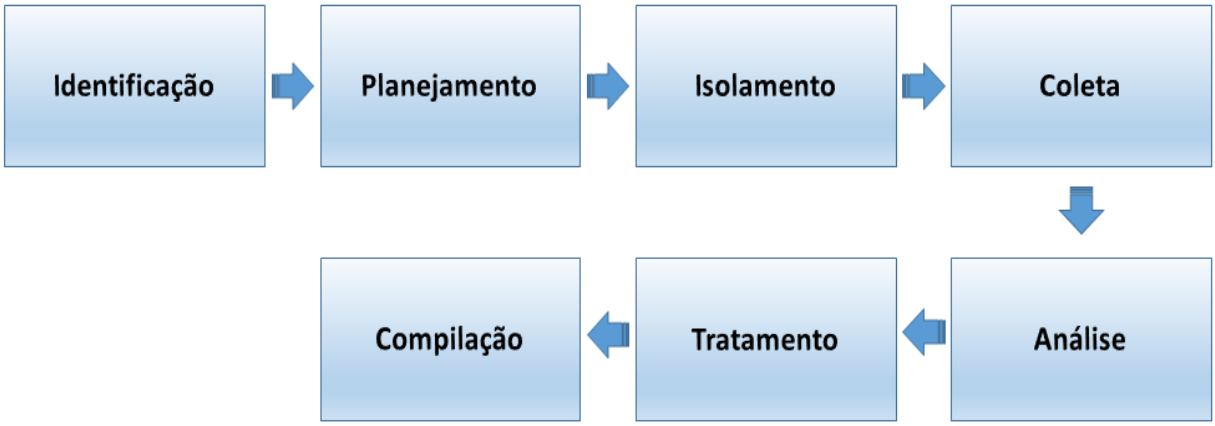
[20] São códigos escritos na maioria das vezes em linguagem *assembly* e têm como missão explorar vulnerabilidades injetando códigos no sistema alvo.

5 MODELO CONCEITUAL

Uma vez levantado o conceito de forense e segurança da informação, a validação deste trabalho se dá pela elaboração de um modelo conceitual partindo deste montante de informação, de modo a estabelecer uma estratégia de perícia para um determinado caso, ou, suspeita de incidente de informação.

A figura 14 descreve tal modelo, e será de vital importância para a execução do método proposto por este trabalho e para o resultado final pretendido pelo autor.

Figura 14 - Modelo Conceitual



Fonte: Autor (2014).

A seguir, cada etapa é detalhada com objetivos e conceitos utilizados para a elaboração do método descrito pela figura 13.

5.1 IDENTIFICAÇÃO

Para a etapa de identificação o foco se volta às necessidades da empresa, aqui, o perito deve definir uma abordagem de definição das frentes necessárias para a elaboração e execução de um plano de ação, e estratégia de investigação (forense estática, dinâmica ou mista), além de conhecer bem o modo de trabalho da empresa, níveis de acesso disponíveis para a investigação, acesso à estação de trabalho, servidores e assim por diante.

Também é importante na etapa de identificação, se estabelecer o primeiro **marco (ou *milestone*)** da investigação. O marco pode ser representado por qualquer informação de peso para a investigação como um todo, podendo variar desde a **data de início e fim da investigação**, quanto a descoberta de alguma evidência contundente, a elaboração do **laudo**, ou seja, qualquer ponto de importância alcançado dentro da investigação que faça com que o perito se aproxime do resultado final.

Para que seja possível o levantamento dessas informações, uma reunião é necessária com o pessoal responsável pela requisição de uma perícia, nesta reunião, os tópicos levantados serão:

- **O que aconteceu.** Aqui é importante que a empresa passe ao perito exatamente o ocorrido (se possível) com datas ou perspectivas do ocorrido (suspeita). Aqui em fase pré-investigativa nada é definitivo ou relevante o suficiente para conclusões, por isso somente dados são levantados para se formarem informações adiante.

- **Quais os danos.** A importância de conhecer o que aconteceu acarreta na direta importância de conhecer o dano pelo qual o perito foi necessário ao caso em questão. Importante frisar que podem não existir danos, muitas vezes a perícia é necessária para averiguar uma suspeita, ao invés de um incidente confirmado e protocolado como doloso à corporação, neste caso, esta etapa abrange a **perspectiva** de danos decorrentes da suposta suspeita. Todavia havendo danos palpáveis, a acurácia do planejamento é significativamente aumentada, tornando o trabalho do perito mais fácil, e de maior confiabilidade.

- **Suspeitas.** As suspeitas refletem no plano de ação do perito como ponto de partida, portanto o argumento da empresa deve ser válido, e embasado o suficiente para que seja de real utilidade e viabilidade para o perito. De posse dos dados obtidos nos tópicos anteriores, o próprio perito pode deduzir uma suspeita e divulga-la (ou não), incluí-la em relatórios e documentações pessoais.

- **Cultura da empresa.** O mais importante da etapa de identificação é conhecer a cultura da empresa. Aqui são levantadas questões a fim de se descobrir **como a empresa trabalha,** quais os costumes esperados dos seus colaboradores, conjunto de normas internas regidas pela corporação, o âmbito de negócios da empresa, **políticas de segurança de informação**, serviços gerais, níveis de acesso de funcionários e assim por diante. Importante que o perito tenha uma ideia completa do funcionamento e estrutura da empresa, para que se possa iniciar um bom planejamento.

5.2 PLANEJAMENTO

A etapa de planejamento se inicia com os dados de identificação do problema levantados, porém esta massa de dados ainda não está devidamente tratada a fim de consolidar uma investigação. Então, a etapa de planejamento compreende os seguintes passos:

- **Compilar os dados levantados.** Unindo a massa de dados em um único documento, possibilita uma melhor análise do que a empresa forneceu.

- **Analisar a compilação de dados.** O perito utiliza de técnicas automatizadas (ferramentas) e do próprio conhecimento e experiência para analisar os dados obtidos a fim de gerar informações vitais para a investigação, separando os dados por relevância, ocorrência, finalidade e utilidade.

- **Definir a estratégia.** Com a compilação de dados analisada pelo perito chega a hora de definir a estratégia de investigação, entende-se por estratégia as técnicas **estática, dinâmica e mista** forense. Este estágio da investigação dita o passo do restante do procedimento, já que a estratégia definida influencia diretamente nos resultados obtidos, e na obtenção de informações sobre o ocorrido, sendo esta etapa a mais importante de todo o modelo elaborado.

- **Definir as ferramentas.** As ferramentas aqui definidas são complementares à definição da estratégia, e diretamente proporcionais ao sucesso da investigação. As ferramentas selecionadas devem abranger o maior ângulo possível de possibilidades, de monitoramento a execução, não havendo número limite de selecionáveis (embora quanto mais bem definida a estratégia, menos ferramentas serão necessárias).

- **Documentar os passos realizados.** Ao final de cada etapa é imprescindível a documentação de todos os passos dados pelo perito até então, num formato de relatório, ou *log* pessoal. Aqui é importante lembrar, que para que a veracidade, credibilidade e validade da investigação, **toda documentação produzida pelo perito deve ser encriptada (recomendado que sejam utilizados algoritmos simétricos para ganho de desempenho), e replicada à múltiplas formas de armazenamento (*backup*).** Feito isso o perito é prevenido de sabotagens externas, e adversidades naturais que podem ocorrer durante a investigação.

5.3 ISOLAMENTO

Como a etapa de isolamento irá proceder depende diretamente da estratégia adotada pelo perito na etapa de planejamento, podendo tomar dois caminhos possíveis.

- **Isolamento da informação.** Aplicado juntamente com a estratégia estática, o isolamento da informação se dá por limitar o *array* de objetos investigados, e diminuir o *range* de falsos positivos, **isolando** a ação do perito em determinado foco (p.ex. uma estação de trabalho, HDs, etc).

- **Isolamento da ação.** Isolar a ação está atrelada à pratica dinâmica de forense, e difere do isolamento de informação, por limitar a esse cenário as técnicas de monitoramento e análise em **tempo real**, como análise de memória volátil, e *logs* de tráfego de rede interno e externo dentro da corporação.

Isolando sua abordagem o perito se beneficia de um **tempo de resposta** adequado com o **problema x abordagem,** quanto menos amplo o quadro de análises diferentes e número de iterações necessária para a investigação, maior o desempenho e precisão do perito quanto à análise do caso e produção do laudo pericial.

5.4 COLETA

O fim do planejamento marca o início da execução. A etapa de coleta se dá pela utilização e execução das ferramentas selecionadas no ambiente isolado, de modo a obter um número suficiente de **dados brutos** a serem analisados e futuramente compilados.

Assim como o isolamento, a coleta pode variar de acordo com a estratégia selecionada pelo perito apresentando características como:

- **Manutenção dos dados coletados.** Em qualquer abordagem os dados coletados devem ser mantidos de modo a preservar a veracidade e credibilidade da investigação. No caso de uma **estratégia estática** é necessário que:

    - **Os dados provenientes das mídias coletadas sejam copiados e encriptados.** Numa investigação forense, qualquer detalhe pode vir a invalidar todo o esforço realizado, assim, o perito deve se preocupar em realizar uma cópia inalterada de toda a massa de dados (*working copy*), além de uma segunda cópia (*work área*) que será a realmente utilizada para a investigação. Essa medida tem por objetivo assegurar a investigação, e sempre se encontrar disponível

uma cópia fiel e **segura** (visto que foi encriptada, e somente o perito possui a chave para decifrar seu conteúdo) possibilitando a investigação de manter seu ponto de partida intacto, além de prover ao perito argumentos que **provem** a possível adulteração dos dados.

- **Criar um perímetro de segurança físico para as mídias coletadas.** Não somente os dados, mas as mídias em si devem ser catalogadas, classificadas e protegidas como fontes de informação. Um perímetro físico **seguro** consiste em camadas de segurança física onde o acesso só é permitido via sequência de **identificações e autenticações** de nível de acesso de pessoal ao local de armazenamento da mídia.

Para a escolha de abordagem dinâmica, os mesmos princípios de manutenção são válidos (múltiplas cópias, cópia inalterada encriptada), não sendo necessário somente o perímetro físico, visto que uma memória volátil só é de utilidade enquanto o sistema está vivo.

- **Documentação das mídias e dados coletados.** Como um anexo a tudo que foi documentado até aqui, o perito deve documentar e catalogar as mídias (forense estática), ou arquivos de *dumps* de memória e *logs* de tráfego de rede (forense dinâmica) compilados em um único documento, relatório ou *log* pessoal, devidamente **encriptados** e replicados.

5.5 ANÁLISE

A etapa de análise tem por objetivo separar as **evidências** da **massa de dados** coletada anteriormente, para isso pode-se fazer uso de ferramentas de análise (definidas na etapa de planejamento) ou utilizando de técnicas pessoais de análise.

Tendo somente a função de separação, a etapa de análise se apresenta como a mais simples, visto que é apenas um trabalho de filtragem, que elimina dados redundantes e irrelevantes da massa, e produz evidências a serem tratadas e compiladas dentro do previsto em lei a fim de se tornarem **provas**.

Ao final desta etapa, o processo deve novamente ser **encriptado** e **replicado** como modo padrão de proteger os passos importantes e fundamentais da investigação.

5.6 TRATAMENTO

Tratar as evidências significa dar sentido **legal** a elas, aqui tem-se dados filtrados em informações de modo a se formarem **evidências** porém ainda não há provas se realmente o incidente é válido, ou até se realmente existiu um incidente na corporação.

Para isso o âmbito legal da investigação entra em vigor, só aqui o perito começa seu trabalho de aplicação da legislação vigente, referências cruzadas com outros casos similares, de modo a reaproveitar vestígios de investigação, materiais produzidos pela mesma e etc.

Tão logo as evidências são tratadas, o perito deve então novamente **encriptar e replicar** o trabalho realizado, além de recompilar todo o trabalho com todos os passos dados e decisões tomadas, a fim de produzir um **laudo, uma prova** que sustente uma conclusão.

5.7 COMPILAÇÃO

A última etapa consiste na produção de um compilado de todo o trabalho do perito até o momento, em formato de relatório de modo a fundamentar o resultado da investigação como **prova.**

O laudo produzido deve possuir um *log* de todo o processo, juntamente com o levantado pelo perito de dados da empresa como um comparativo dado-a-dado, políticas de

segurança adotadas, em resumo, um *backtrack* de toda a investigação e de todos os resultados obtidos.

Para que tenha validade a prova deve ser incontestável, por isso a preocupação em proteger essas informações deve ser uma constante durante a investigação, pois leis possuem brechas, e o processo de investigação é delicado o suficiente para que seja facilmente invalidado, principalmente se o alvo de investigação é um cargo de confiança dentro da corporação (presumindo que as suspeitas sejam contra o gerente de TI da empresa, por exemplo) o número de tentativas de invalidação do laudo pode vir a ser muito grande, para isso a investigação deve ser conduzida com cautela, e com o máximo de exatidão, não deixando nenhum detalhe de lado, visto que qualquer deslize reflete diretamente na veracidade e validade do laudo, e da própria investigação.

6 EXECUÇÃO DO MODELO EM ESTUDO DE CASO

O modelo proposto no capítulo 5 sugere uma investigação forense em sete etapas que se complementam de acordo com a evolução da mesma, e para que seja posto em prática, este modelo necessita de um cenário montado com a intenção de ilustrar como se aplicam as ferramentas selecionadas, como uma investigação segue de acordo com o planejado, e, por fim, como o apanhado de evidências se transforma em **provas** que podem inocentar ou culpar um indivíduo, ou corporação.

Visto isso, o cenário a seguir foi elaborado pelo autor com o objetivo de abordar um incidente de **vazamento de informação** em uma empresa contratante do ramo de desenvolvimento de *software*, sendo este um problema de natureza **ordinária** e que pode ocorrer direta, ou indiretamente de dentro ou fora da empresa contratante, **anteriormente** ao início da investigação, ou seja, o incidente já foi identificado e precisa ser tratado e investigado de modo que a empresa contratante possa tomar as medidas legais cabíveis a este caso.

6.1 IDENTIFICAÇÃO, ENTENDENDO O PROBLEMA

Identificar o problema é o primeiro e mais importante passo da investigação, já que o perito necessita de um entendimento completo do que vai investigar dentro da empresa. Aqui como explicado no modelo, são levantadas todas as informações relevantes e cabíveis ao caso em questão, de modo a reduzir o número de falsos positivos, desvios de foco, evidências inconsistentes, e replanejamento.

A etapa de identificação se inicia imediata a realização da primeira reunião com os representantes da empresa contratante, o que define o primeiro **marco** da investigação, sendo este a **data de início da investigação**. Para fins de dimensionamento temporal e melhor situação de tempo e espaço, o autor define a data de início da investigação como dia **20 de maio de 2014**, produzindo o primeiro dado da investigação.

Dando continuidade à reunião, o perito deve prosseguir ouvindo o que a empresa contratante tem a dizer sobre o incidente em questão mediante uso de um simples questionário, que direciona a reunião para as necessidades reais do perito, que se concentram em saber **o que aconteceu**, **quais as suspeitas da empresa contratante sobre o suposto incidente, como a empresa trabalha (qual a cultura adotada na empresa), e, por fim, como a empresa está estruturada**.

Após a apresentação deste questionário, a reunião procede com a empresa contratante basicamente respondendo às questões propostas e levantando suas necessidades e expectativas quanto à investigação em questão.

Ao se aplicar o questionário, as respostas obtidas foram:

- **Qual o incidente suposto? (Qual o problema investigado, o que aconteceu?)** Como explicado anteriormente, trata-se de um **vazamento de informação**, mas que informação? Identificado pela empresa contratante, o incidente se caracteriza pela percepção de um módulo novo implementado no software da empresa concorrente, equivalente a um mesmo módulo implementado, porém ainda não em produção, presente no software proprietário da empresa.
    - **Variável:** Se o módulo supostamente vazado ainda não está em produção no *software* da empresa, pode ser caracterizado o furto de informação?
        - **Problema:** Provar qual empresa **desenvolveu** o módulo primeiro. Não se pode levar em conta o código-fonte puro, somente o fluxo lógico da aplicação, visto que o código pode sofrer fatorações que alteram a estrutura do código mas não mudam o fluxo lógico da aplicação, o que significa que o mesmo código pode estar escrito de **n** formas, mas ainda funcionar da mesma maneira e apresentar os mesmos resultados, mensagens, validações e relatórios que não invalidam a cópia.
    - **Variável:** Se ambos os *softwares* são destinados ao mesmo segmento de mercado, ramo de clientes, e público-alvo, a presença de um módulo comum não pode ser caracterizada como vazamento, e sim como uma solução comum entre os dois.

- **Quando a empresa identificou o incidente? (Neste caso, pretende-se descobrir exatamente quando a empresa contratante percebeu o suposto vazamento).** Para esta pergunta o cliente informou a data 11 de maio de 2014, estabelecendo assim o segundo **marco** da investigação, sendo este a **data de detecção do problema por meio do cliente**.
    - **Variável:** Um período de 09 dias entre a data de detecção e início da investigação dá tempo hábil (caso seja possível provar o vazamento) aos envolvidos em vazar a informação de cobrir seus rastros e danificar equipamentos que podem ter sido utilizados para a propagação da informação.
        - **Problema:** O tempo do suposto vazamento não é equivalente a 09 dias, portanto aqui é necessário saber quanto tempo o desenvolvimento do módulo supostamente vazado levou para ser desenvolvido e testado. De posse dessas informações podem ser aplicados filtros de modo a facilitar a investigação como, por exemplo:
            - Se o módulo supostamente vazado não está em produção pela empresa contratante, deve possuir alguma falha lógica (*bug*), sendo assim, pode-se se testar o *software* produzido pela concorrente a fim de verificar se os mesmos problemas ocorrem, em caso positivo, pode-se tirar deste a primeira **evidência** de **vazamento de informação**. Aqui a empresa contratante informa que o módulo em questão levou 4 meses para ser desenvolvido.

- **Quem são os envolvidos no desenvolvimento do software?** Esta pergunta tem por objetivo encurtar os espaços da investigação “travando” os alvos investigados aos envolvidos diretamente no desenvolvimento. Para isso, a empresa contratante informou que a equipe de desenvolvimento do software é formada por 10 integrantes, sendo divididos em:

- 5 desenvolvedores
- 1 designer
- 2 analistas
- 1 gerente
- 1 *tester*
- **Variável:** Por mais que se conheça a equipe de desenvolvimento, não se pode ter certeza de que somente estes têm acesso ao código-fonte. Sendo assim, por mais que a investigação seja focada nos envolvidos **diretamente** no desenvolvimento, caso não haja levantamentos e evidências conclusivas, deve-se levantar posteriormente os envolvidos **indiretamente** com o *software*, sendo pessoas de acesso ao armazenamento do mesmo, podendo englobar tanto diretores, quanto o próprio responsável pela infraestrutura ou profissionais de segurança da informação e banco de dados da empresa contratante, e, por serem cargos de confiança, podem dificultar a investigação.
    - **Problema:** Isolar a investigação de modo que cada membro da equipe tenha seu envolvimento com o código esclarecido, e buscar meios de não necessitar a abrangência da investigação a outros colaboradores da empresa contratante, o que pode prejudicar a precisão dos dados levantados, atrasar a produção de resultados, e dar vasão por consequência para a contestação e repúdio aos resultados futuramente coletados, analisados e tratados provenientes da investigação.
- **Variável:** Quando o módulo foi pensado? A razão por trás desta dúvida se dá pela noção temporal e espacial necessárias ao perito para conduzir a investigação. Aqui é importante que a empresa revele a data da primeira reunião, ou primeiro *brainstorming* correspondente a esse módulo. Qual a sua gênese, quando ele foi bolado? Para esta pergunta, a empresa revela que a primeira reunião com o módulo em pauta ocorreu em **05 de Outubro de 2013.**

- **Quais as políticas de segurança adotadas pela empresa?** Esta pergunta tem por objetivo conhecer **como a empresa trabalha**, sendo de vital importância para o bom desenvolvimento da investigação. Aqui necessitam ser conhecidos todos os dados referentes aos costumes e a cultura adotada pela empresa contratante, de modo que o perito possa conhecer os perímetros de segurança adotados na empresa, o nível de acesso que ele terá dentro de suas dependências, os tipos de equipamentos com ferramentas detalhadas pertinentes a cada um dos envolvidos e listados como membros da equipe de desenvolvimento do *software* em questão. Explicado o motivo da questão, a empresa contratante informa que:
    - Quanto aos costumes, e perímetros de segurança:
        - O uso de mídias de armazenamento removível e portátil é **permitido** a todos os colaboradores.
        - Todos os colaboradores possuem acesso **irrestrito** à internet.
        - O controle de entrada e saída é realizado por uma catraca eletrônica ligada a um sistema controlador que armazena cada ação disparada pela mesma. Ou seja, para se adentrar na empresa, cada colaborador ou visitante deve ser identificado e autenticado. Neste caso pode-se ter mais segurança, embora nada possa ser garantido, de que somente circula na empresa contratante quem faz parte do quadro de colaboradores, ou é visitante reconhecido, previamente combinado, e acompanhado, limitando o acesso livre de **estranhos** nas dependências da empresa.
        - O tráfego da rede é monitorado pelo colaborador responsável pela segurança da informação dentro da empresa contratante.
        - A empresa utiliza de um serviço de *e-mail* próprio, logo, todo o fluxo de dados é monitorado, identificado, e “logado” de modo a se produzir um histórico de envio, recebimento e anexo de documentos por colaborador.

- Quanto aos equipamentos e ferramentas utilizadas pelos colaboradores da empresa contratante:
    - A empresa possui um misto de *notebooks* e *desktops* rodando sistema operacional *Microsoft™ Windows®* 7 *Ultimate* de 64bits.
        - **Problema:** No caso da empresa contratante trabalhar com *notebooks*, deve-se esclarecer se os colaboradores que fazem uso deste equipamento podem retirá-los das dependências da empresa contratante, sejam por motivos de **reuniões na sede de clientes, ou para *home office.*** A relevância desta informação se dá pelo intervalo de tempo que **a estação de trabalho não estará conectada na rede interna da empresa,** podendo prejudicar a investigação por falta de informações nos *logs* posteriormente coletados da rede.
    - Para armazenamento, a empresa possui um servidor próprio de banco de dados, baseado em PostgreSQL.
    - Para controle de versionamento, é adotada a tecnologia SVN[21].
    - O monitoramento de conteúdo de navegação é feito através da utilização de um *firewall* de autenticação[22] com relatórios gerados pelo uso da ferramenta SARG[23].
    - Todos os desenvolvedores da empresa utilizam a ferramenta Eclipse *Juno* para codificação.

---

[21] SVN é a abreviação de *subversion*, é um controlador de versões com o objetivo de armazenar em servidor versões de arquivos com históricos de alterações "logadas" por usuários com permissão *read and write*, ideal para ações em grupo, onde muitas pessoas alteram o mesmo arquivo múltiplas vezes. Servindo também como *backup* e restauração. Tendo aplicações práticas para revisão e correções, permitindo o retorno a uma versão anterior de um determinado dia, ou hora.

[22] Também conhecido como *firewall* autenticado, tem por característica o *login* ou seja, para se iniciar a navegação, cada usuário deve ser identificado e autenticado, e uma vez autenticado, seus dados de navegação possuirão seus dados cadastrais como identificadores.

[23] Abreviação para *Squid Analysis Report Generator*, é uma ferramenta que permite ao usuário da tecnologia a visualização de navegação completa de um usuário da rede. Gerando um HTML contendo informações como **identificação de usuários, endereços IP, bytes enviados e recebidos na transação de conexão, quais *sites***

- Para documentação e especificação de *software* os analistas utilizam a ferramenta *Enterprise Architect* 9.0.
- Para desenvolvimento de protótipos, os *designers* fazem uso das ferramentas Adobe™ *Photoshop* CS6

- Quanto ao nível de acesso do perito, a empresa contratante concordou em:
  - Acesso ilimitado com data de acesso pré-definida às:
    - Estações de trabalho dos membros da equipe de desenvolvimento, com intervalo de pelo menos 1 dia entre estações.
    - *Logs* diários gerados pelo *firewall* da empresa via SARG.
    - *Logs* produzidos pela catraca eletrônica.

Com os dados fornecidos pela empresa, o perito tem as informações necessárias para começar o processo de planejamento e definir o rumo do restante da investigação.

6.2 PLANEJAMENTO, DEFININDO UM RUMO

Finalizada a reunião com os representantes da empresa contratante, tem-se o questionário respondido com as anotações do perito quanto aos problemas, variáveis de caso, o perito já conhece o problema, sabe também qual seu papel dentro da empresa, como a empresa trabalha, qual a cultura adotada, e qual o acesso liberado para desempenhar sua função de investigador.

Agora, como manda o modelo elaborado no capítulo 5, deve-se analisar o levantado na etapa de identificação, **cifrar e replicar** o questionário respondido com as anotações do perito, e definir as ferramentas necessárias para os próximos passos da investigação.

---

foram acessados e estampas de tempo de acesso, segundo informações retiradas do *website:* sourceforge.net/projects/sarg/.

6.2.1 Analisando o levantamento de dados sobre o possível incidente

Segundo os dados reunidos, a empresa contratante observou um possível vazamento de informação de código-fonte de um determinado módulo de seu produto. Para isso foi anotado que esta observação ocorreu 09 dias antecessores à data de início da investigação.

Agora, com a finalidade de se montar uma noção temporal e espacial, o perito leva em consideração o período da primeira observação da empresa contratante de **09 dias,** e acrescenta **4 meses** (tempo de desenvolvimento do módulo informado pela empresa) a fim de se montar um perímetro temporal para o procedimento da investigação. Sendo o resultado desta soma, o período de **11 de Janeiro de 2014 a 20 de Maio de 2014.**

Além disso, acrescenta-se o período de concepção desse módulo, sendo levado em consideração que qualquer *brainstorming* produz dados, que podem ser fundidos de modo a se produzir conhecimento, que catalogado e documentado, pode vir a ser material vazado. Então, o novo início do perímetro temporal da investigação se torna dia **05 de Outubro de 2013**, sendo esta a data da primeira reunião realizada para se definir as funcionalidades e o propósito deste módulo.

Sendo assim, tem-se um período de investigação de **07 meses e 15 dias**, período este relativamente grande, que necessita ser investigado com cautela, pois a massa de dados produzida será de grande quantidade, aumentando a chance de algum dado ou informação não ser observado com o cuidado devido, podendo em longo prazo prejudicar os resultados da investigação e até gerar retrabalho considerável.

O próximo ponto a se observar é a quantidade de *logs* que o perito tem acesso, desde o controle de versionamento da empresa, até as estações de trabalho de cada membro da equipe de desenvolvimento. Tendo-se tantas frentes para se “atacar” o perito deve pensar agora na estratégia viável para o procedimento posterior da investigação.

6.2.2 Definindo estratégias de investigação

Visto no capítulo 4 deste trabalho, uma investigação forense pode ter caráter **estático** ou **dinâmico** dependendo do que se pretende investigar, e do estado das informações coletadas que se tem sobre o cenário proposto.

Pela duração do perímetro temporal, é mais adequada a aplicação da estratégia de investigação **estática** visto que quase a totalidade do material de investigação serão *logs* e discos, com a efetuação de *ghosts* de discos rígidos, análises de código fonte, *dumps* de memória, relatórios gerados pelo SARG, etc.

No entanto, deve-se sempre partir do seguinte cliché "o criminoso sempre volta à cena do crime", então medidas preventivas devem ser tomadas de modo a reforçar as evidências em caso de novas tentativas de vazamentos de informação, então para monitoramento e análise em **tempo real**, pode-se aplicar a estratégia de investigação forense **dinâmica**. Aqui é possível observar algumas variáveis quanto ao suposto vazamento, como:

- **Modo de propagação**, tendo em vista que a empresa permite que seus colaboradores façam uso livre de mídias de armazenamento portáteis (HDs externos, *pendrives*, *smartphones*, etc.), e todos os colaboradores possuem acesso irrestrito à internet, o modo de propagação já possui várias ramificações, o que pode fazer com que a investigação demore mais tempo do que deveria ou poderia, tendo em vista que **somente** levando em consideração a propagação *online* via *e-mail* pode gerar algumas possibilidades, sendo essas:
    - O *e-mail* utilizado foi **externo** (provedor extra-empresa) ou **interno** (fornecido pela empresa).
    - Os arquivos anexados podem estar cifrados, ou fragmentados, gerando esforço muito maior para quebrar a chave, ou desfragmentar o arquivo de modo a se dar sentido à informação, demandando ainda mais esforço, e tempo, tempo que nem sempre está disponível para o perito utilizar na investigação.

Após definidas as estratégias, o próximo passo proposto é definir as ferramentas da investigação.

6.2.3 Definindo ferramentas

Definidas as estratégias da investigação, o perito deve começar a pensar em quais ferramentas utilizar para a execução adequada da estratégia adotada.

Analisando o que foi levantado, o perito julgou pertinente a abordagem estratégica **estática** e **dinâmica**. Levando em consideração definir as ferramentas é o momento mais importante da investigação, tendo em vista que as ferramentas influenciam diretamente no desempenho, acurácia, credibilidade e validade da investigação.

Visto isso, as ferramentas são definidas como:

- Para a área de trabalho do perito, é necessário um **notebook** limpo (entende-se por limpo, um *notebook* com sistema operacional recém-instalado e sistema de arquivos em padrão de fábrica, onde não existe nenhum arquivo pessoal do perito, tampouco arquivos decorrentes da investigação) e homologado pela empresa contratante.

    - Importante frisar que o como uma investigação forense dentro de uma corporação lida com informações delicadas para a empresa contratante, o sigilo da manipulação dessas informações necessita ser previstas em contrato ou em acordo homologado por ambas as partes, por isso, o *notebook* necessita ser formatado, limpo e homologado no **início** e no **fim** da investigação. Desse modo, é assegurada a confidencialidade das informações investigadas, coletadas, analisadas e tratadas durante a investigação.

        - Quanto ao sistema operacional escolhido, o perito acha mais vantajoso utilizar o sistema operacional *Windows* 8.1, com distribuição Linux Kali 1.0.6 virtualizada via *Oracle Virtual Box*.

- Quanto ao uso do equipamento listado, importante frisar que o *notebook* **não** fica conectado a rede interna da empresa contratante, sendo utilizado apenas para análise de dados coletados.

- Como a maior parte dos dados de coleta já virão diretamente da empresa contratante, como relatórios do SARG, *logs* de *firewall*, servidor de *e-mails*, e *logs* de SVN, código fonte a ser analisado, e a própria função do sistema operacional que fornece todas as informações relevantes ao estado do sistema de arquivos, é importante ressalvar que não serão necessárias para este caso, ferramentas específicas para coleta de dados. Para *ghosts* e *dumps* serão utilizadas funções nativas dos sistemas operacionais, como citado no capítulo 4.

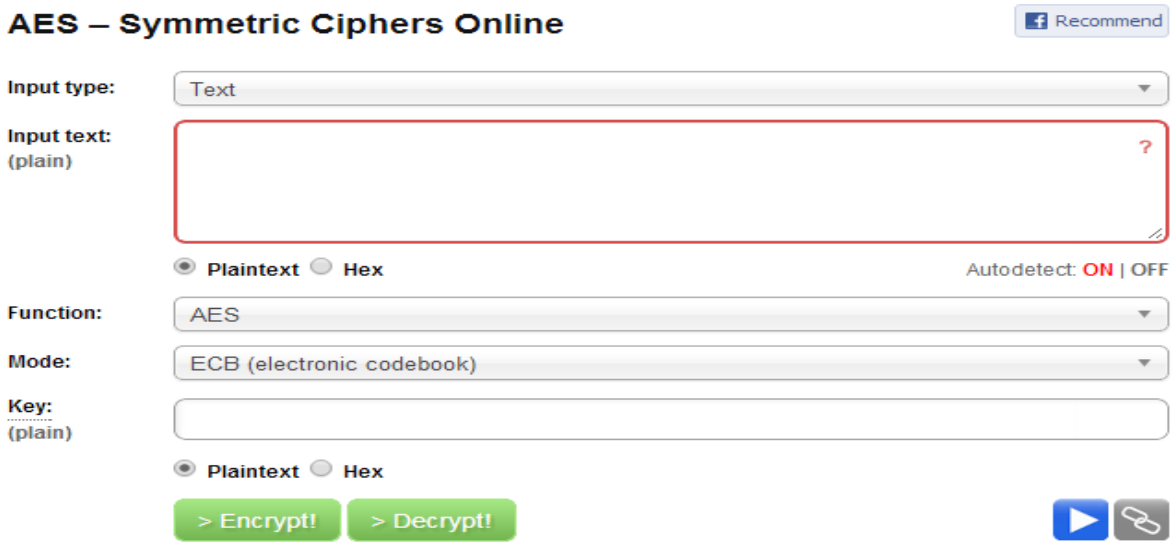
- Para monitoramento e realização de forense dinâmica, é interessante utilizar o *WIRESHARK* em conjunto ou não com o *RETINA* ficando como opção extra. A função deste é monitorar o tráfego da rede de modo a acusar novas tentativas de vazamento, verificar "lixo" dentro do *log* de tráfego, e capturar tentativas de conexão por máquinas pertencentes a topologia de rede da empresa contratante.

- Para cifrar os dados da investigação, o perito utilizará a ferramenta grátis *online AES – Symmetric Ciphers Online*, disponível em: <http://aes.online-domain-tools.com>.
    - Escolhida cifra simétrica pelo ganho em desempenho e na confidencialidade de somente o perito ter acesso à chave simétrica.

    - A escolha desta ferramenta em particular se dá pela liberdade do perito em escolher a função de cifra (AES, DES, 3DES, etc.), escolher também o tipo de *input* (arquivo ou texto plano), como ilustrado na figura 15 o *layout* e as funcionalidades básicas do *software*, como mostrado, pode-se escolher cifrar um texto claro, ou um arquivo de texto, escolher o tipo de algoritmo a ser aplicado,

o modo de execução do algoritmo selecionado, e então, ao clicar em *encrypt* o texto cifrado é produzido e disponibilizado para o perito, desta forma o processo de cifra e replicação se torna mais performático e viável. Também pode-se observar que o processo inverso pode ser executado, inserindo o texto ou arquivo cifrado com a chave selecionada (para este trabalho, a palavra-chave selecionada foi "forense"), a ferramenta produz o mesmo texto claro.

Figura 15 - AES *Symmetric Ciphers Online*



Fonte: http://aes.online-domain-tools.com/

Para finalizar a etapa de planejamento da investigação, como previsto pelo modelo conceitual elaborado no capítulo 5, o perito deve cifrar todas as informações originadas da identificação e do planejamento, e replicá-las como forma de *backup* de tudo o que foi feito.

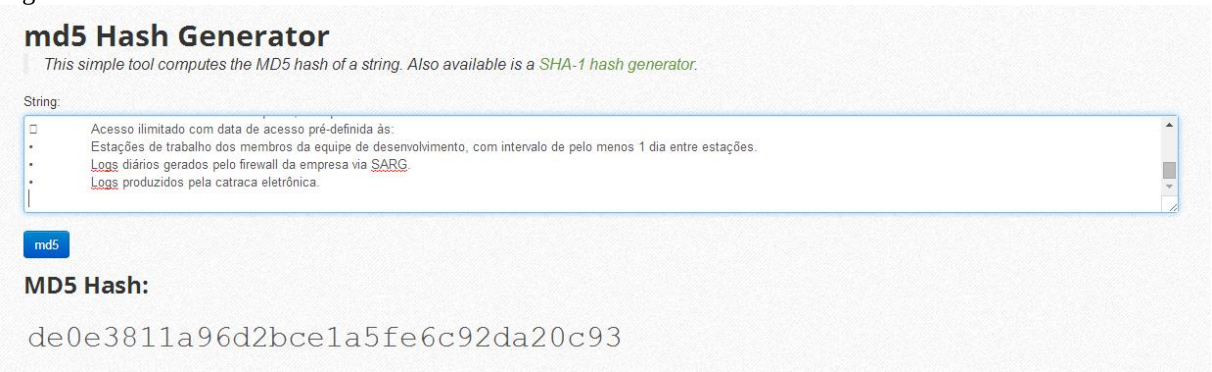
Para ilustrar como isto é feito, todo o presente neste trabalho de investigação no capítulo 6 será encriptado utilizando o AES *Symmetric Ciphers Online*, utilizando a palavra-chave "forense" para o processo de cifra simétrica (APÊNDICE A – Trecho de texto cifrado utilizando AES – *Symmetric Ciphers Online*).

Uma vez o texto cifrado, o modelo sugere que se gere um *hash* a fim de garantir a **integridade** de todos os resultados que a investigação produzir. Para isso, é definida uma ferramenta *online* geradora de *hash* MD5 chamada *MD5 HASH GENERATOR*, fácil de

utilizar, esta ferramenta difere pouco do AES *Symmetric Ciphers Online*, não necessitando de uma chave, somente o texto que será resumido via *hash*.

E como mostra a figura 16 o *hash* gerado é disponível para cópia, e será anexado com o texto cifrado.

Figura 16 - MD5 *HASH GENERATOR*



Fonte: http://www.miraclesalad.com/webtools/md5.php

Feito o procedimento de cifra, replicação, e *hash*, a etapa de planejamento se encontra finalizada, podendo continuar a investigação isolando a área de investigação e aplicação das estratégias aqui definidas.

6.3 ISOLAMENTO: ISOLANDO A ÁREA DE INVESTIGAÇÃO E APLICAÇÃO DE ESTRATÉGIAS

Para definir as “áreas” isoladas na investigação, ou os **pontos de isolamento da investigação**, tem-se as informações do perímetro temporal, ou seja, a período de **05 de Outubro de 2013 a 20 de Maio de 2014** serve como primeiro parâmetro de isolamento, desse modo, a investigação será isolada neste período sendo este o foco da posterior coleta de dados.

O próximo parâmetro a ser levado em consideração para a investigação é a **equipe de desenvolvimento** do *software* em questão, dado que também foi levantado na etapa de identificação da investigação.

Então, o isolamento desta investigação será efetuado da seguinte forma:

- A coleta de dados será referente ao período de **05 de Outubro de 2013 a 20 de Maio de 2014.**

- Dentro deste período, somente serão coletados dados referentes à equipe de desenvolvimento envolvida no *software* que supostamente teve suas informações vazadas ao concorrente. Neste caso, os dados buscados são:
    - Registro da catraca eletrônica da empresa contratante dentro destes **pontos de isolamento da investigação**. (A fim de se verificar os dias exatos que cada um dos membros da equipe estava na empresa, e futuramente utilizar dos mesmo para referências cruzadas na etapa de análise).
    - *Logs* do servidor de *e-mails* referentes aos **pontos de isolamento da investigação**.
    - *Logs* do *firewall* da empresa contratante, reforçando a necessidade de ser somente referente aos **pontos de isolamento da investigação.**
    - Relatórios gerados pelo SARG.
    - Informações do estado do sistema de arquivos de cada estação de trabalho.
    - Análise dos códigos-fonte do *software*.
    - Análise dos históricos do SVN referentes aos **pontos de isolamento da investigação**.

Chegando ao final da etapa de isolamento, as informações referentes à esta etapa são cifradas, replicadas, e um *hash* é gerado. Neste caso o perito utiliza o texto produzido no APÊNDICE A - Trecho de texto cifrado utilizando AES – *Symmetric Ciphers Online*, com o hash produzido e ilustrado na figura 15.

6.4 COLETA: COLETANDO MASSA DE DADOS

A etapa de coleta tem como ponto de partida e referência os dados levantados na etapa de identificação, ferramentas definidas na etapa de planejamento e o(s) ambiente(s) definido(s) no isolamento.

Tendo em vista que a empresa contratante fornece a maioria dos dados necessários para a investigação, a etapa de coleta tem como primeiro objetivo estabelecer a ordem em que as informações serão coletadas junto a empresa.

Como o vazamento de informação pode ser efetuado de várias maneiras, é importante classificar qual meio de vazamento é mais relevante para cada situação. Desse modo o perito pode dividir a investigação de modo a exercer o isolamento previsto.

Sendo assim fica definida a ordem de coleta como:

- Histórico de envios de *e-mails*, incluindo histórico de arquivos anexados recuperados diretamente da base de dados referente ao serviço de *e-mail*. (APÊNDICE B – *Logs* de *e-mails* enviados pela equipe de desenvolvimento).
- *Logs* do *firewall* e SARG.
- Histórico de mudanças do SVN.
- Coleta de informações do sistema de arquivos de cada estação de trabalho.

A etapa de coleta não ignora nenhum dado, a massa a princípio é totalmente relevante e válida para o caso, o momento de filtragem e classificação dessa massa fica caracterizado como **análise.**

6.5 ANÁLISE: SEPARANDO AS EVIDÊNCIAS DA MASSA DE DADOS

Como definido pela etapa de coleta, a primeira massa de dados a se observar e analisar é o histórico de envios de *e-mails*, mas o que o perito está realmente procurando neste

histórico? Sabe-se que os dados já estão filtrados pelo que foi isolado, então as datas de envio já estão corretas, o que se precisa observar aqui é o assunto do *e-mail*, conteúdo, e principalmente anexos, e qual o endereço de envio do *e-mail* em questão para que se possa confirmar o vazamento da informação **para a empresa concorrente**.

Analisando os *logs* disponíveis, o perito se depara com um *e-mail* enviado no dia **10 de Dezembro de 2013** por um dos desenvolvedores à empresa concorrente contendo 1 arquivo no formato. rar sendo segundo o colaborador, a **primeira parte** do combinado. (APÊNDICE C – *E-Mail* Capturado à empresa concorrente)

Este *e-mail* explicitamente vazando informações sigilosas da empresa contratante consolida este envio como **evidência** de tal vazamento, visto que os arquivos se tratam de:

- Código-fonte até então produzido
- Arquivos de especificação gerados pela empresa contratante
- Descrição de algoritmos do módulo vazado.

Diante disto, aplica-se um filtro para a listagem de *e-mails* enviados do colaborador analisado pelo **endereço de envio**, obtendo-se uma segunda lista de *e-mails* enviados somente à empresa concorrente (APÊNDICE D – Lista de *e-mails* enviados à empresa concorrente).

Visto a lista de *e-mails* observa-se então que o colaborador em questão enviou 15 *e-mails* com os mesmos arquivos anexados à empresa concorrente, fazendo com que se possa concluir que a empresa concorrente **contratou** o vazamento de informação diretamente da equipe de desenvolvimento no decorrer de tempo hábil para se replicar o módulo em seu *software*.

A fim de se consolidar a evidência, uma segunda lista é levantada sendo essa a lista de *e-mails* recebidos do desenvolvedor com origem da empresa concorrente confirmando o recebimento do material, e informando do devido pagamento pela tarefa executada (APÊNDICE E – Lista de *e-mails* enviados ao colaborador pela empresa concorrente).

6.6 TRATAMENTO: APLICANDO LEIS ÀS EVIDÊNCIAS ANALISADAS

Com a **evidência** de que a empresa concorrente contratou de fato a colaboração de um dos desenvolvedores da empresa contratante, o próximo fato é desvendar se isso é realmente justificado como **crime**, praticado tanto pelo desenvolvedor quanto pela empresa concorrente, de modo a se validar a investigação efetuada até o momento.

Tem-se em mãos a listagem de *e-mails* recebidos e enviados referentes ao código fonte, especificação, algoritmos, e informações de pagamento pela informação vazada, para que essas evidências sejam apresentadas como provas de um crime, se aplicam as seguintes leis como mostra Bolzan Júnior (2011):

- **Violação do segredo profissional** - Artigo 154 da legislação brasileira
    - **Art. 154** – Revelar a alguém, sem justa causa, segredo, de que tem ciência em razão da função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem:
        - **Pena** – detenção, de 3 (três) meses a 1 (um) ano, ou multa.

- **Furto** – Artigo 155 da legislação brasileira
    - **Art. 155** – Subtrair, para si ou para outrem, coisa alheia móvel:
        - **Pena** – reclusão, de 1 (um) a 4 (quatro) anos, e multa.
        - **§ 1º** - A pena aumenta-se de um terço, se o crime é praticado durante o repouso noturno.
        - **§ 2º** - Se o criminoso é primário, e o objeto furtado é de pequeno valor, o juiz pode substituir a pena de reclusão pela de detenção, e diminuí-la de um a dois terços, ou aplicar somente a pena de multa.

- **Roubo** – Artigo 157 da legislação brasileira
    - **Art. 157** - Subtrair coisa móvel alheia, para si ou para outrem, mediante grave ameaça ou violência a pessoa, ou depois de havê-la, por qualquer meio, reduzido à impossibilidade de resistência:
        - **Pena** – reclusão, de 4 (quatro) a 10 (dez) anos, e multa.

- **§ 1º** - Na mesma pena incorre quem, logo depois de subtraída a coisa, emprega violência contra pessoa ou grave ameaça, a fim de assegurar a impunidade do crime ou a detenção da coisa para si ou para terceiro.

- **Estelionato** – Artigo 171 da legislação brasileira
  - **Art. 171** - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento:
    - **Pena** - reclusão, de 1 (um) a 5 (cinco) anos, e multa.
    - **§ 1º** - Se o criminoso é primário, e é de pequeno valor o prejuízo, o juiz pode aplicar a pena conforme o disposto no Art. 155, § 2º.
    - **§ 2º** - Nas mesmas penas incorre quem:
      - **I** - vende, permuta, dá em pagamento, em locação ou em garantia coisa alheia como própria;
      - **II** - vende, permuta, dá em pagamento ou em garantia coisa própria inalienável, gravada de ônus ou litigiosa, ou imóvel que prometeu vender a terceiro, mediante pagamento em prestações, silenciando sobre qualquer dessas circunstâncias;
      - **III** - defrauda, mediante alienação não consentida pelo credor ou por outro modo, a garantia pignoratícia, quando tem a posse do objeto empenhado.
      - **IV** - defrauda substância, qualidade ou quantidade de coisa que deve entregar a alguém;
    - **§ 3º** - A pena aumenta-se de um terço, se o crime for cometido em detrimento de entidade de direito público ou de instituto de economia popular, assistência social ou beneficência.

- **Violação de direito autoral** – Artigo 184 da legislação brasileira
    - **Art. 184 -** Violar direitos de autor e os que lhe são conexos:
        - **Pena -** detenção, de 3 (três) meses a 1 (um) ano, ou multa.
        - **§ 1º** - Se a violação consistir em reprodução total ou parcial, com intuito de lucro direto ou indireto, por qualquer meio ou processo, de obra intelectual, interpretação, execução ou fonograma, sem autorização expressa do autor, do artista intérprete ou executante, do produtor, conforme o caso, ou de quem os represente:
            - **Pena -** reclusão, de 2 (dois) a 4 (quatro) anos, e multa.
            - **§ 2º -** Na mesma pena do § 1º incorre quem, com o intuito de lucro direto ou indireto, distribui, vende, expõe à venda, aluga, introduz no País, adquire, oculta, tem em depósito, original ou cópia de obra intelectual ou fonograma reproduzido com violação do direito de autor, do direito de artista intérprete ou executante ou do direito do produtor de fonograma, ou, ainda, aluga original ou cópia de obra intelectual ou fonograma, sem a expressa autorização dos titulares dos direitos ou de quem os represente.

Com as evidências tratadas legalmente, o modelo propõe que o perito execute todas as medidas de segurança (cifra, replicação e hash) e compile todas essas informações de modo a se formar provas.

6.7 COMPILAÇÃO: ELABORAÇÃO DE PROVAS

Para finalizar a investigação, as informações aqui levantadas são reunidas de modo a:

- **Pela divulgação ilegal** do produto desenvolvido na empresa contratante, com início no dia **10 de Dezembro de 2013** conforme levantado pelos históricos de *e-mails* enviados e recebidos pelo desenvolvedor da equipe de desenvolvimento do *software* em questão, enquadra-se o próprio como ação **criminosa** dentro do previsto em lei pelos artigos 154, 155, 157, 171 e 184 da constituição em exercício na república federativa do Brasil.

- A continuação da prática criminosa pelos subsequentes meses configura repetição contínua de tal ato doloso à empresa contratante em prática deliberada pelo período de **10 de Dezembro de 2013 (Data referente ao primeiro envio de informação)** a **13 de Maio de 2014 (Data do último envio de informação para a empresa concorrente),** acumulando no delito em questão as penas enquadradas em cada artigo mencionado, de modo cumulativo a serem aplicadas em conformidade com cada caso.

- A investigação tem como resultado **positivo** quanto ao vazamento de informação suspeitado pela empresa contratante, por meio consensual entre a empresa concorrente e o desenvolvedor colaborador da empresa, por intermédio do serviço de *e-mail* interno da empresa contratante, sendo representados como dados vazados **código-fonte, arquivos de especificação e algoritmos específicos de regras de negócio**.]

Finalizada a compilação da investigação, o perito pode então **provar** à empresa contratante que um determinado incidente ocorreu de fato, ou não, sempre bom lembrar que esta etapa serve também para que o perito mostre com precisão tudo o que foi feito durante a investigação por meio de artefatos produzidos por ele mesmo, de modo a se poder realizar um *backtracking,* ou seja, se estabelecer um ponto de retorno caso seja necessário um novo ciclo de investigação, e também guardar tais artefatos como bibliotecas e referências para uma nova investigação em cenário similar.

7 CONCLUSÃO

O cenário aqui descrito foi planejado de modo a se validar o modelo proposto por este trabalho como um modelo de investigação forense viável e válido para ambientes corporativos. Para isto o cenário foi controlado de modo a se produzir resultados rapidamente visto que o tempo disponível para tal realização era escasso.

O que foi provado nesta investigação é que houve de fato um vazamento de informação, porém ainda não foi provado que a empresa concorrente utilizou este código-fonte, para isso seria necessário:

- Mandato judicial para investigação similar dentro do ambiente corporativo da empresa concorrente.

- Teste aplicado ao software concorrente para se estabelecer se os mesmos *bugs* relatados para o produto da empresa contratante ocorrem no produto da empresa concorrente. O que pode vir a gerar evidências ainda mais contundentes do uso de informação vazada.

- Eventos corriqueiros como uma simples queda de energia pode acarretar em danos significativos para a investigação no caso de análise **dinâmica**.

- A empresa contratante pode não estar disposta a liberar o acesso do perito a todas as informações dentro de seu ambiente de trabalho.

- O vazamento pode ter sido causado por transporte em mídias de armazenamento removíveis, o que dificulta o plano e ângulo de ação do perito, pois não se pode dizer que foi o próprio colaborador usufrutuário da área de trabalho onde a mídia foi colocada a fim de copiar as informações quem de fato efetuou a cópia para divulgação ilícita.

- O trabalho de apreensão de tais itens deve ser feito somente mediante ordem judicial, que pode demorar mais do que se é conveniente e interessante para a investigação.

- Em ambiente real, várias complicações e variáveis podem vir a aparecer como:
    - A empresa concorrente pode ter obtido acesso via rede.
    - O *e-mail* pode ter sido enviado de um servidor externo, sendo de mais difícil acesso.
    - Mesmo que sejam descobertos tais *e-mails*, os anexos podem ser **cifrados** e **fragmentados** o que obriga o perito a resgatar todas as partes do arquivo, desfragmentar, decifrar o arquivo (vale a observação de que não se sabe como essas informações foram cifradas), e submeter este arquivo a novas análises de modo a se concluir se o que está sendo transmitido é de fato relevante à investigação e também se é de fato, informação sigilosa ou de autoria da empresa contratante.
    - Ferramentas necessitam ser instaladas na rede interna da empresa, de preferência uma que se restringe somente ao rastreamento de informação, e uma segunda que sinaliza, ou analisa a informação capturada, a fim de se registrar uma nova tentativa de acesso externo.

Além disso, essa investigação se limitou aos *e-mails* vistos a praticidade da aplicação de tal consequência, agora, em um ambiente real seria realmente necessária a investigação de cada uma das áreas de trabalho, com *dumps* para auxiliar a investigação, preferencialmente com a apreensão das HDs por um período determinado.

Por fim observa-se a facilidade com o que a investigação inteira pode ser invalidada, caso qualquer um dos dados seja interceptado, ou alterado, por isso a constante utilização de *hash* para garantir a **integridade** de todo o material produzido.

7.1 TRABALHOS FUTUROS

Uma vez alcançados os objetivos deste trabalho, visto que o tempo de execução e os fatores de tempo, capacitação técnica e esforço não puderam ser realmente aplicados

devido à simulação de investigação em ambiente empírico e controlado, ficam como trabalhos futuros:

- A evolução do modelo proposto de modo que evolua sua dinâmica e capacite ainda mais sua viabilidade.

- Amadurecer o modelo proposto de modo que possa atender toda e qualquer divergência que ocorra em um ambiente real em situação verídica não só de vazamento de informação mas de furtos, ou *cyber* crimes em geral.

- Aplicar o modelo amadurecido em um ambiente corporativo, ou governamental.

- Estabelecer com este modelo, um padrão investigativo que auxilie o autor na carreira de sua escolha como perito forense.

- Desenvolvimento próprio de *softwares* que trabalhem *off-line* na criptografia dos dados levantados referentes à investigação.

Restam ainda algumas considerações finais referentes a esse trabalho.

7.2 CONSIDERAÇÕES FINAIS

Embora seja possível identificar o uso da legislação vigente do país para crimes digitais, também é possível observar a **falta** de leis específicas para essa área no Brasil, sendo necessária a reformulação ou extensivas interpretações para que se possa formar um conceito válido para **provar** a ocorrência ou não de um incidente. Este fato pode dificultar em muito o trabalho de um perito forense, e pode fazer com que o trabalho exigido que já é complexo e extensivo fique bem mais extenso e complexo, além de possibilitar múltiplas abordagens legais que podem invalidar todo o trabalho realizado.

Exatamente por isso, países emergentes e “novas economias” como o Brasil precisam estabelecer seu próprio conjunto de leis específicas para a informática, de modo a desencorajar praticantes de crimes virtuais, diminuir ou extinguir a impunidade para tais atos, e facilitar o trabalho de perícia e investigação.

Porém, mesmo com esta ressalva, foi constatado então que os objetivos propostos por este trabalho foram de fato alcançados, visto que a aplicação do modelo conceitual foi bem sucedida embora em ambiente controlado e empírico, e os conceitos de segurança da informação foram bem aplicados de modo a se consolidar uma prova de vazamento de informação por intermédio de um colaborador da empresa contratante via *e-mail* interno da própria empresa, mediante acordo com a empresa concorrente, o que lesou o contratante por violação de direitos autorais, e pela concorrente fazer uso e liberação para acesso em produção antecipadamente ao próprio dono do código, conceito, concepção, usufruto e lucro, resultando em uma pena acumulada de pelo menos 29 anos de reclusão, ou multa, dependendo do julgamento do juiz.

REFERÊNCIAS

AIRES, João Paulo. **Tipos de pesquisa (Características e Exemplos) CNPq.** Universidade Federal do Paraná, 2003. Disponível em: < http://pessoal.utfpr.edu.br/joao/arquivos/Aula%203%20-%20Tipos%20de%20Pesquisa,%20Curriculum%20Lattes.pdf > Acesso em 23 out. 2013.

ALVES, André Luiz; ALVES, Fabrício Silva. **Aplicabilidade dos Principais Conceitos de Segurança no Ciclo de Vida de Sistemas em S*oftware Houses***. Goiás, Goiania, 2009.

ARBAUGH, William A. *et. Al*. ***Windows of Vulnerability: A Case Study Analysis***. USA, 2000.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Tecnologia da informação – Técnicas de segurança – Código de prática para gestão da segurança da informação NBR ISO/IEC 17799.** Rio de Janeiro, Rio de Janeiro, 2005.

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

BOLZAN JÚNIOR, Juvenal. **Legislação aplicada à informática – Livro didático.** Universidade do Sul de Santa Catarina, Palhoça, Santa Catarina, 2011.

BORAN, Sean. ***IT Security Cookbook***. USA, 1996, Disponível em: < http://www.boran.com/security/> Acesso em 01 out. 2013.

CAMPOS, André. **Sistemas de Segurança de Informação: Controlando os Riscos**. 2. Ed. / André Campos. Florianópolis: *Visual Books*, 2007.

CARVALHO, Luciano Gonçalves. **Segurança de Redes**. Rio de Janeiro: Editora Ciência Moderna Ltda., 2005.

CARUSO, Carlos A.A; STEFFEN, Flavio Deny. **Segurança em informática e de informações.** Editora SENAC, 1999.

CAVALLARO, Dani; ***Cyberpunk & Cyberculture: Science Fiction and the Work of William Gibson.*** *Bloomsbury Academic; 1st edition,* 2000.

GOMES, Kleiton da Silva e Santos, Newton. **Segurança no Desenvolvimento de Aplicações WEB**. Amazonas, Universidade da Amazônia – UNAMA – Centro de Ciências Exatas e Tecnológicas – CCET – Trabalho de Conclusão de Curso de Bacharel em Ciência da Computação, 2006.

CANDIDO, Arnaldo Júnior; SAÚDE, Almir Moreira. **Técnicas e Ferramentas Utilizadas em Análise Forense**. UNESP – Universidade Estadual Paulista, campus de São José do Rio Preto, 2005.

FAGUNDES, Leonardo Lemes; **Gestão de riscos em segurança da informação.** UNISINOS, 2008.

GIAVAROTO, Silvio César Roxo; SANTOS, Gerson Raimundo dos. ***BackTrack* Linux – Auditoria e Teste de Invasão em Redes de Computadores.** Rio de Janeiro, Editora Ciência Moderna Ltda., 2013.

GURJAR, Chintan. ***Computer Forensic – A case study – InfoSec suite*.** Artigo eletrônico, disponível em: < http://resources.infosecinstitute.com/computer-forensics-investigation-case-study/>, 2013.

KLEIN, Daniel V. ***Improving System Security via Proactive Password Checking***. USA, 1995.

LAUREANO, Marcos Aurelio Pchek; MORAES, Paulo Eduardo Sobreira. SEGURANÇA COMO ESTRATÉGIA DE GESTÃO DA INFORMAÇÃO. **Revista Economia & Tecnologia**, São Paulo, v.8, n.3, p.38-44, 2005.

LENTO, Luiz Otavio Botelho. **Governança e Gestão da Informação,** Livro Digital Universidade do Sul de Santa Catarina, Palhoça, 2010.

LYRA, Maurício Rocha. **Segurança e Auditoria em Sistemas de Infomação,** Rio de Janeiro: Editora Ciência Moderna Ltda., 2008.

MADEIRA, Mauro Notarnicola. **Forense Computacional,** Livro Digital Universidade do Sul de Santa Catarina, Palhoça, 2012.

MARTINI, Renato. **Criptografia e cidadania digital**. Rio de Janeiro: Editora Ciência Moderna Ltda., 2001.

MARTINS, Elaine. **O que é cracker – Desvendando os Mistérios dos "Piratas Virtuais"**. Disponível em: < http://www.tecmundo.com.br/o-que-e/744-o-que-e-cracker-.htm >

MENEZES, Alfred; OORSCHOT, Paul van; VANSTONE, Scott. ***Handbook of Applied Cryptography***. 2.ed. USA, 1996.

MRDOVIC, Sasa et al. ***Combining Static and Live Digital Forensic Analysis in Virtual Enviroment***. Artigo científico, *Faculty of Electrical Engineering, University of Sarajevo.* Sarajevo, Bosnia e Herzegovina, 2011.

OLIVEIRA, Fábio Borges. **Análise de Segurança de Criptografia e Esteganografia em Seqüências de Imagens**. Petrópolis, Rio de Janeiro, 2007.

OLIVEIRA, Salomão. **Segurança e Gestão da informação**. Apostila digital do curso de Gestão de Tecnologia, Disciplina de "Normas e Políticas de Segurança da Informação". Centro Universitário Radial Estácio, Jabaquara, São Paulo, 2008.

PASHEL, Brian A. ***Implications in Teaching Students to Hack at the University Level***. USA, 2008

PINHEIRO, Reginaldo César. **Os cybercrimes na esfera jurídica brasileira**. **Jus Navigandi**, Teresina, ano 5, n. 44, 1 ago. 2000. Disponível em: <http://jus.com.br/artigos/1830>. Acesso em: 28 jun. 2014.

Leia mais: http://jus.com.br/artigos/1830/os-cybercrimes-na-esfera-juridica-brasileira#ixzz36BiKW1Mx

QUEIROZ, Leonardo Bastos. **O SGSI e o ciclo PDCA.** 2012 Disponivel em: < http://www.leonardobastos.com.br/1/post/2012/03/clusulas-mandatrias-42-estabelecendo-e-gerenciando-o-sgsi.html >. Acesso em 08 out 2013.

ROUSE, Margaret. **What is *zero-day* exploit?** Disponível em: <http://searchsecurity.techtarget.com/definition/zero-day-exploit>. Acesso em 21 mar 2014.

SCHUBA, Cristoph L. et al. ***Analysis of a Denial of Service Attack on TCP***. *West Lafayette, Indiana, USA,* Editora: *Purdue E-pubs,* 1996.

SIQUEIRA, Marcelo Costa. **Gestão estratégica da informação.** Brasport, 2005.

SPANCESKI, Francini Reitz. **Política de Segurança da Informação: Desenvolvimento de um modelo voltado para Instituições de Ensino**. Joinville, Santa Catarina, 2004

STALLINGS, Willian. **Criptografia e segurança de redes: Princípios e práticas.** *Prentice Hall,* 4th edition, 2002.

STEPHENSON, Peter. ***eEye Digital Security Retina Network Security Scanner***. *SCMagazine digital for IT Security Professionals*. Artigo digital. Disponível em: < http://www.scmagazine.com/eeye-digital-security-retina-network-security-scanner/review/3081/> Acesso em 30 mar 2014.

SUHAIL, Ansari et.Al. ***Packet Sniffing: a brief introduction***. USA, Editora *Potentials,* 2.ed 2003.

TÁLAMO, Maria de Fátima G; SMIT, Moreira; Johanna W. **Ciência da informação: Pensamento Informacional e Integração Disciplinar.** São Paulo: *Brazilian Journal of Information Science*, 2007. Também disponível em: <http://http://www2.marilia.unesp.br/revistas/index.php/bjis/article/viewFile/30/29> . Acesso em: 24 ago. 2013.

TAVARES, Diego. **Forense Computacional**. Seminário digital, PET Computação, UFCG, 2010.

URUPOJ, Kanlayasiri et. Al. ***A Rule-based Approach for Port Scanning Detection***. *Applied Network Research Group, Department of Computer Engineering, Faculty of Engineering, Kasetsart University, Chatuchak, Bangkok, Thailand,* 2002.

WADLOW, Thomas. **Segurança de Redes**. Editora Campus. Rio de Janeiro, Rio de Janeiro 2000.

APÊNDICES

APÊNDICE A – Trecho de texto cifrado utilizando AES – *Symmetric Ciphers Online*

O primeiro apêndice mostra o resultado de um texto cifrado utilizando a ferramenta AES – *Symmetric Ciphers Online*.

O processo se deu por:

- Copiar o que foi descrito da etapa de identificação
- Colar o texto no campo de texto na ferramenta
- Selecionar o algoritmo AES em ***function***
- Selecionar ECB (*eletronic codebook*) em ***mode***
- Digitar a palavra chave “forense” na tela, no campo *key*.
- Clicar em “*encrypt*”
- Após o processo de encriptação finalizado, clicar em *download binary file*
- O texto produzido então fica da seguinte maneira.


```
¾ŸDÍÃK&p_þ—Ó,îÎãC¤x÷"ÅÚ8-□€v_àC3¤PuC_Ê
u;¼Õ† l¥□KÙñš.£Õj_Ç”U'„÷†}5o„"]I|5HrW_*9!v_
Šv_ÞÙ$□øª_„µ_j’b1ã^Ô_Å Uw‘7õÍ¯F˜±îÍDF»ã-
Ò¼ÓrB_ÕVÀÙ±_°lCjô2x□S’õ¯qÜÁZÍC"³□ô
_ËáG¨ì
^÷Íð□ÐUåt ¾«lÎ†©_Úó”šŒ¤"_Ä_ôã€4¥-MGëóV'0-ä-°ÅcÛÙ4|c´_vÇ8+jD•f_2
q%_Æ¾! Ã[iÊ§¨»_Q_üsû`r_=²—›ËÖ_{SŸ`½¦†¿³DŸÃÔu’9·ê±_^ð•
□˜_×0À[;Ë‹tÝt’-
^Å%«Y› `NÁqþ_`ìù#öJÝRXÓ,ØœÐC__{_±°òÁ□¡†~E°Ö_êÇKšf¨Ú2¡_C©7ÙÆSM”U,Á_¼Ò
õ_™Š•VT”__¥Îùø□_$1ÃÕCaõþ·F_¿˜__½„õÂ_Î ,{|g*_aÑ1_^¦eè…_ëê3dÜBÁ^¾•R•KÁ
YU•?*yÚ_ôe°Ø? 2Ÿ_ë_/-^·š_„5´#ß¿ìAwÓÁ□yYVû³ðŒ¸0)8n‘¦x-4«_€A›Ê
Dóhz%]CZ°˜÷ÉN›æš_□~ÉS□âûõ_d°€P³v±ŠÅ¼f®áÇT_¼¿ÖaS_31o …,L_£F;}□□Æœ
Œ¦®_%aHÏ_Õ_ª@RfÒFÆœ_Ç¤9N½_}$ %û`ÉsáH|´Ç;óÞÇoBœ
Œ¦®_%aHÏ_Õ_ª@R·žW2'%M«ŸÕ´
_ôÓ¿w”_€®_]ÎŒ:‘Õ(P¼o_þ°7“œ__¶[mås_PAÖK_éuûÒRúå¶É-ªˆÈ1W_ _Ï:Î© £Ü
¸V“hû_á8»8_1ƒˆ±f½Ãçù_¦í€y“_!_w_Ÿ2óÌ-
¢o„•ZË™mMK__…^Þ‹ˆE_ÄlÝœ_G_CZö¹^HlŒ+_q_:^Û_ö¢__18¤Ý.M‰ÂV_|_Üûò^’³UJÅÕ
Œ¿úîö u+fç.Â□…LB-
Ýa³bÏöì;cÑ#ŽàTHÅ_¸‡‘_uf¼=Ï2‘œ_ÔÜj¢‹°ú©õ_¾V§_\÷X›ÖFß‰B9I§š‡¯k4ê•tÇyål
_†g×c·>ƒò3@jQœ_°6Kóâ/^wÉÞ¿à‹øŠâk*ãK¶}-œ1â¯¾.Éú’7_¿š”u‹*6±_VÙ8
_V__b□0»R+.ðvç’ÁšÎèÜƒÎ…KçP□œ
□F‘KúéñeeÅK.À*(ÍWR□Ò¢Ló˜_%]"
?=V□ÆJ¡ó[&©_±_VX,_'Iî À?ïü5æ~E«Ág]_j_¸ï__“¥9Â_@=ÎÇÏ7æÒZ`ÅA}Tò%••°¯úæ
]_
éÕêI_Û‘oJî-
½Fy!OžP.W__ü¥…»Å om□¤€__UÉÞ*§AÿE„\_mú&•□ÒgV{Þëg“7!*ü*žD._YžÒÑŸ__Ó;àû
*ó‰oøbã„ZÀðô»¨Ü£ÎÑ.%b_}%8<àgC„ÝÃ>{xÁ»
Ltä¹S□__ÅË□î9%q…ðR_šŠ›ø¶□K`™ü_8a□ÁÑA”be9ûD…žÕPñ·ú;ùE°ÎH___¼
r_Ó~Þwûl}!:1Ô_#ç †_ì˜æ_§ÆM58Ú8ªˆd:ã?^___7ç¢3Ö5=èÅ-0_¾ Â_õ
„_wv_nf»"wÔ]_Ž_ÐèÄ®ÜóeBùt>¼_ùëaA0ý_À1¾B]&þd
```

APÊNDICE B – *Logs* de *e-mails* enviados pela equipe de desenvolvimento

De:	Para:	Assunto:	Data de envio
desenvolvedor1@empresa.com.br	contato@email.com.br	ASSUNTO	05/10/2013
desenvolvedor2@empresa.com.br	contato@email.com.br	ASSUNTO	06/10/2013
desenvolvedor3@empresa.com.br	contato@email.com.br	ASSUNTO	07/10/2013
desenvolvedor4@empresa.com.br	contato@email.com.br	ASSUNTO	08/10/2013
desenvolvedor5@empresa.com.br	contato@email.com.br	ASSUNTO	09/10/2013
designer@empresa.com.br	contato@email.com.br	ASSUNTO	10/10/2013
analista1@empresa.com.br	contato@email.com.br	ASSUNTO	11/10/2013
analista2@empresa.com.br	contato@email.com.br	ASSUNTO	12/10/2013
tester@empresa.com.br	contato@email.com.br	ASSUNTO	13/10/2013
gerente@empresa.com.br	contato@email.com.br	ASSUNTO	14/10/2013
desenvolvedor1@empresa.com.br	**contato@empresaconcorrente.com.br**	**Sem assunto**	**10/12/2013**
desenvolvedor2@empresa.com.br	contato@email.com.br	ASSUNTO	11/12/2013
desenvolvedor3@empresa.com.br	contato@email.com.br	ASSUNTO	12/12/2013
desenvolvedor4@empresa.com.br	contato@email.com.br	ASSUNTO	13/12/2013
desenvolvedor5@empresa.com.br	contato@email.com.br	ASSUNTO	14/12/2013
designer@empresa.com.br	contato@email.com.br	ASSUNTO	15/12/2013
analista1@empresa.com.br	contato@email.com.br	ASSUNTO	16/12/2013
analista2@empresa.com.br	contato@email.com.br	ASSUNTO	17/12/2013
tester@empresa.com.br	contato@email.com.br	ASSUNTO	18/12/2013
gerente@empresa.com.br	contato@email.com.br	ASSUNTO	19/12/2013
desenvolvedor1@empresa.com.br	contato@email.com.br	ASSUNTO	20/12/2013
desenvolvedor2@empresa.com.br	contato@email.com.br	ASSUNTO	21/12/2013
desenvolvedor3@empresa.com.br	contato@email.com.br	ASSUNTO	22/12/2013
desenvolvedor4@empresa.com.br	contato@email.com.br	ASSUNTO	23/12/2013
desenvolvedor5@empresa.com.br	contato@email.com.br	ASSUNTO	24/12/2013
designer@empresa.com.br	contato@email.com.br	ASSUNTO	25/12/2013
analista1@empresa.com.br	contato@email.com.br	ASSUNTO	26/12/2013
analista2@empresa.com.br	contato@email.com.br	ASSUNTO	27/12/2013
tester@empresa.com.br	contato@email.com.br	ASSUNTO	28/12/2013
gerente@empresa.com.br	contato@email.com.br	ASSUNTO	29/12/2013

APÊNDICE C – *E-Mail* Capturado à empresa concorrente

APÊNDICE D – Lista de *e-mails* enviados à empresa concorrente

De:	Para:	Assunto:	Data de envio
desenvolvedor1@empresa.com.br	**contato@empresaconcorrente.com.br**	**Sem assunto**	**10/12/2013**
desenvolvedor1@empresa.com.br	**contato@empresaconcorrente.com.br**	**Sem assunto**	**10/01/2014**
desenvolvedor1@empresa.com.br	**contato@empresaconcorrente.com.br**	**Sem assunto**	**22/02/2014**
desenvolvedor1@empresa.com.br	**contato@empresaconcorrente.com.br**	**Sem assunto**	**19/03/2014**
desenvolvedor1@empresa.com.br	**contato@empresaconcorrente.com.br**	**Sem assunto**	**30/04/2014**
desenvolvedor1@empresa.com.br	**contato@empresaconcorrente.com.br**	**Sem assunto**	**13/05/2014**

APÊNDICE E – Lista de *e-mails* enviados ao colaborador pela empresa concorrente

De:	Para:	Assunto:	Data de envio
contato@empresaconcorrente.com.br	**desenvolvedor1@empresa.com.br**	**Sem assunto**	**11/12/2013**
contato@empresaconcorrente.com.br	**desenvolvedor1@empresa.com.br**	**Sem assunto**	**11/01/2014**
contato@empresaconcorrente.com.br	**desenvolvedor1@empresa.com.br**	**Sem assunto**	**23/02/2014**
contato@empresaconcorrente.com.br	**desenvolvedor1@empresa.com.br**	**Sem assunto**	**20/03/2014**
contato@empresaconcorrente.com.br	**desenvolvedor1@empresa.com.br**	**Sem assunto**	**31/04/2014**
contato@empresaconcorrente.com.br	**desenvolvedor1@empresa.com.br**	**Sem assunto**	**14/05/2014**