Computação forense aplicada a crimes cibernéticos no Judiciário federal

Computer forensics applied to cyber crimes in the federal Judiciary

Marina Alves Ferreira*

Artigo recebido em 27/01/2022 e aprovado em 15/06/2022.

Resumo

O objeto de estudo deste artigo é o fluxo de tratamento de incidentes cibernéticos envolvendo ilícitos, ou seja, tipificados como penalmente relevantes, no Judiciário federal. Observando o contexto atual do cenário brasileiro, há uma tendência de aumento de ataques cibernéticos a vários órgãos do governo em todas as esferas e, decorrente disso, a publicação de legislações com diretrizes para padronização do tratamento de incidentes cibernéticos, a fim de propiciar o aumento da maturidade dos órgãos nesse assunto. O artigo apresenta vários conceitos definidos por autores renomados para estabelecer um nivelamento sobre os termos utilizados nos protocolos analisados. Por fim, serão vistos o detalhamento das legislações e o fluxo dos protocolos correlacionados com o uso da computação forense. Conclui-se que tais legislações são norteadoras para os órgãos e propiciam o amadurecimento organizacional deles com relação ao assunto.

Palavras-chaves: segurança da informação; tecnologia da informação; programa de computador; ambiente cibernético; crime.

Abstract

The object of study of this article is the flow of treatment of cyber incidents involving illicit, that is, typified as criminally relevant, in the federal judiciary. Observing the current context of the Brazilian scenario, there is a tendency to increase cyber attacks on various government agencies in all spheres and, as a result, the publication of legislation with guidelines for standardizing the treatment of cyber incidents in order to provide an increase in maturity of the bodies in this matter. The article presents several concepts defined by renowned authors to establish a leveling on the terms used in the analyzed protocols. Finally, the detailing of legislation and the flow of protocols correlated with the use of computer forensics. It is concluded that such legislations are guiding the bodies and provide the organizational maturation of the same in relation to the subject.

Keywords: information security; information technology; computer program; cyber environment; crime.

1 Introdução

Com o passar dos anos, a tecnologia mostrou-se fundamental para comunicação, trabalho, transações e muitas outras atividades que ocorrem no mundo, tornando-se uma necessidade básica para a sociedade. Manuel Castells, autor do livro "A sociedade em redes", previu o impacto da tecnologia da informação na sociedade e seus desdobramentos. Ele criou vários conceitos, como "capitalismo informacional" — o qual define que a informação se tornou o bem mais valioso na sociedade em rede. Também definiu o conceito de "espaços de fluxos", que descreve o tipo de espaço que torna possível a interação à distância em tempo real e de forma síncrona, prevendo a influência da internet e do ciberespaço na sociedade. Como toda evolução, há pontos positivos e negativos, por exemplo, "todos estão interconectados em escala global o que favorece a comunicação" (CASTELLS, 1999), mas também a

* Graduada em ciência da computação pelo Centro de Ensino Unificado de Brasília –UniCEUB. Pós- graduada, *latu senso*, em gestão e infraestrutura de serviços de TI, pela Faculdade Juscelino Kubitschek. MBA em computação forense pelo Instituto de Pós-graduação e Graduação – IPOG. Servidora do Tribunal Regional Federal da 1ª Região.

ocorrência de crimes cibernéticos nos quais atacantes enxergam o usuário ou provedor do serviço como potenciais vítimas.

E o que seriam crimes cibernéticos?

> *Crime cibernético* – ato criminoso ou abusivo contra redes ou sistemas de informações, seja pelo uso de um ou mais computadores utilizados como ferramentas para cometer o delito ou tendo como objetivo uma rede ou sistema de informações a fim de causar incidente, desastre cibernético ou obter lucro financeiro (PRESIDÊNCIA DA REPÚBLICA, 2021).

Devido à pandemia provocada pelo covid-19, governos pelo mundo todo optaram por criar regras para controlar o fluxo de pessoas nas ruas. Logo, o teletrabalho tornou-se a solução e a nova realidade para muitas empresas. Contudo, ao fornecer o acesso remoto aos servidores e aplicações das organizações por meio de VPNs[1] para o usuário, elas também se tornaram mais vulneráveis a ataques cibernéticos. Rolfini, autora do artigo publicado pelo *site* Olhar Digital (2020), cita o levantamento realizado pela Kaspersky no qual identificaram que os ataques direcionados a ferramentas de acesso remoto subiram 333% em 2020[2].

O alerta feito pelo ministro relator Vital do Rêgo, do Tribunal de Contas da União – TCU, demonstra seu entendimento sobre a questão da segurança nos órgãos públicos brasileiros: "Com a evolução tecnológica e o aumento da digitalização dos serviços públicos, as vulnerabilidades e as falhas de segurança da informação em sistemas relevantes podem afetar significativamente o Estado e os cidadãos" (SECOM TCU, 2021). Ele também demonstrou preocupação devido ao aumento dos ataques cibernéticos e citou como exemplo os casos do Superior Tribunal de Justiça – STJ, Ministério da Saúde, Conselho Nacional de Justiça – CNJ e Governo do Distrito Federal – GDF.

Decorrente desse cenário, o Conselho Nacional de Justiça – CNJ e o Conselho de Justiça Federal – CJF publicaram resoluções e portarias a fim de tratar sobre o tema, além de fornecer diretrizes para adequação de todo o Judiciário brasileiro a regras básicas de segurança da informação e tratamento de incidentes, incluindo aspectos da computação forense ao processo.

Neste artigo serão abordadas normas da ABNT referentes à segurança da informação, a Resolução 396 do CNJ, a Portaria 162 do CNJ, a Portaria 68 do CJF e a Resolução 687 do CJF. Esses normativos formam a base para o tratamento da segurança cibernética na Justiça Federal.

2 Segurança da informação e sua relação com a segurança cibernética

Segundo a norma ISO/IEC 27000 (2018), segurança da informação é a preservação da confidencialidade, integridade e disponibilidade da informação, mas também existem outras propriedades como autenticidade, não repúdio e confiabilidade que também podem estar envolvidas. As três primeiras propriedades citadas também são conhecidas como tríade CIA (sigla em inglês) ou CID (sigla em português) e estão diretamente ligadas à ideia de incidentes de segurança da informação e segurança cibernética.

Já a segurança cibernética é uma vertente da segurança da informação e é definida no glossário de segurança da informação da Presidência da República como:

> *Segurança cibernética* – ações voltadas para a segurança de operações, visando garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético, capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis (PRESIDÊNCIA DA REPÚBLICA, 2021).

Pensando no contexto da segurança cibernética, Velho (2016) traz em seu livro o ponto de conexão entre ela e a aplicação da computação forense, como mostra o trecho abaixo.

---

[1] Sigla de *Virtual Private Network*, em português, Rede Privada Virtual, é uma forma de estabelecer uma conexão protegida, através do uso de criptografia do tráfego de internet, utilizando redes públicas e dificultando o rastreamento das atividades e roubo de dados por terceiros.

[2] ROLFINI, Fabiana. Cibercrime: ataques no Brasil aumentam mais de 300% com a pandemia. *Olhar Digital*. São Paulo, jul. 2020. Disponível em: https://olhardigital.com.br/2020/07/03/seguranca/cibercrime-ataques-no-brasil-aumentam-mais-de-300-com-a-pandemia/. Acesso em: 30 out. 2021.

> As ações de Segurança Cibernética são essenciais, pois é através delas que são postos em prática os serviços de resposta a incidentes e de detecção de intrusão, junto à verificação de conteúdo e à Computação Forense, que é responsável pela análise de todos os vestígios e registros relacionados a um incidente (VELHO, 2016, p. 507).

A fim de alinhar o entendimento e tratamento da Justiça Federal de 1° e 2º graus a respeito da segurança da informação, o Conselho de Justiça Federal – CJF publicou a Resolução CJF 6, de 7 de abril de 2008, a qual foi alterada pela Resolução CJF 687, de 15 de dezembro de 2020, que versa sobre a Política de Segurança da Informação e a utilização dos ativos de informática no âmbito do Conselho e da Justiça Federal de 1° e 2º graus. Entre os tópicos do documento consta a gestão de incidentes de segurança da informação, e é nesse ponto que a segurança cibernética irá atuar diretamente.

2.1 Fundamentos de segurança cibernética

Para melhor entender a segurança cibernética, é importante conhecer a definição de espaço cibernético.

> *Espaço cibernético* – espaço virtual composto por um conjunto de canais de comunicação da internet e outras redes de comunicação que garantem a interconexão de dispositivos de TIC e que engloba todas as formas de atividades digitais em rede, incluindo o armazenamento, processamento e compartilhamento de conteúdo além de todas as ações, humanas ou automatizadas, conduzidas através desse ambiente (PRESIDÊNCIA DA REPÚBLICA, 2021).

O espaço cibernético pode refletir situações das relações humanas, ou seja, em um momento traz proteção, em outro é utilizado de forma ofensiva usando a internet a fim de obter recursos e vantagens ilícitas ou indevidas.

As formas de atuação da segurança cibernéticas são divididas por Velho (2016) da seguinte forma:

- Preventiva: ações para evitar/coibir ameaças cibernéticas. Ex.: *hardening*, troca de equipamentos, melhoria no desenvolvimento de software (programação).
- Reativa: ações de correção de vulnerabilidade e/ou tratamento de um incidente.

As duas formas de atuação têm sua importância no contexto da segurança cibernética, mas segundo um ditado muito usado nessa área, "existem dois tipos de empresas, aquelas que foram invadidas, e aquelas que ainda não sabem que foram". Dito isso, as ações preventivas são importantes, mas não suficientes para a segurança cibernética. Também são necessárias ações reativas, visto que permitem corrigir vulnerabilidades identificadas sobre os ativos e implementar ações de resposta a incidentes. A detecção de um incidente somada à aplicação da computação forense permitirá a análise dos vestígios e registros associados ao incidente de segurança, propiciando a preservação, a coleta e o processamento dos dados.

2.2 Ações dos conselhos de justiça

Inicialmente o CNJ publicou as Portarias CNJ 290, 291 e 292 (protocolos), além das Resoluções CNJ 360, 361 e 362, as quais dispunham sobre a base para um fluxo de tratamento de incidentes cibernéticos e a necessidade de adequação dos órgãos do Judiciário brasileiro a esses normativos. Entre as ações determinadas, estava a criação de um Plano de Ação de Segurança Cibernética pelos órgãos de justiça. O CJF, juntamente com os Tribunais Regionais Federais (TRFs), criou o plano com as ações, prazos e responsáveis definidos. Esse plano foi publicado na Portaria CJF 68.

Contudo, houve uma consulta pública e, após algumas sugestões e avaliações, todos esses normativos publicados pelo CNJ foram revogados e substituídos pela Resolução CNJ 396, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), e pela Portaria CNJ 162, que aprova protocolos e manuais criados pela Resolução CNJ 396/2021. Ambos foram publicados em junho de 2021.

Portanto, além dos protocolos publicados anteriormente, foram acrescidas informações como o detalhamento da Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ) e os manuais presentes na Portaria 162, ambos com o intuito de melhorar o nível de maturidade em segurança cibernética pelos órgãos do Poder Judiciário.

3 Gestão de incidentes cibernéticos e a legislação no Judiciário federal

Para entender como gerenciar um incidente, é necessário observar o cenário que propicia esse evento. O primeiro passo nesse processo é saber que a segurança da informação possui algumas propriedades e que entre as principais estão a confidencialidade, a integridade e a disponibilidade. Ao violar uma dessas propriedades, incorrerá em um incidente de segurança. Além dessas propriedades, as definições de riscos aceitáveis ou não pelo negócio também impactam na definição do que será identificado como incidente e no seu tratamento. Por exemplo, ativos possuem vulnerabilidades que serão exploradas por ameaças e seu tratamento ocorrerá ou não baseado no risco para o negócio definido pela alta gestão. Esse risco é estimado pelo impacto e probabilidade do evento acontecer.

Segundo a norma ABNT ISO/IEC 27001 (2013), a gestão de incidentes de segurança da informação tem como objetivo garantir a eficácia e a consistência no gerenciamento dos incidentes, além da comunicação de vulnerabilidades e de eventos de segurança da informação. Esse gerenciamento é composto por um conjunto de processos para detectar, relatar, avaliar, responder, tratar e aprender com os incidentes de segurança da informação.

Porém, a gestão de incidente de segurança da informação é apenas uma parte do escopo da norma de sistema de gestão de segurança da informação (SGSI). Atualmente, a norma ABNT ISO/IEC 27035-3 trata exatamente da gestão de incidentes focada nas diretrizes para operações de resposta a incidentes de tecnologia da informação, além de contemplar também os controles estabelecidos pela norma ABNT ISO/IEC 27001.

Na figura 1, são apresentadas as fases de gestão de incidentes de segurança da informação segundo a norma ABNT ISO/IEC 27035-1, sendo que a norma ISO/IEC 27035-2 abrange as caixas em laranja (“Planejamento e preparação” e “Lições aprendidas”) e a norma ABNT ISO/IEC 27035-3 abrange as três fases restantes que estão em azul e são coletivamente conhecidas com operações de resposta a incidentes (“Detecção e geração de relatórios”, “Avaliação e decisão” e “Respostas”).

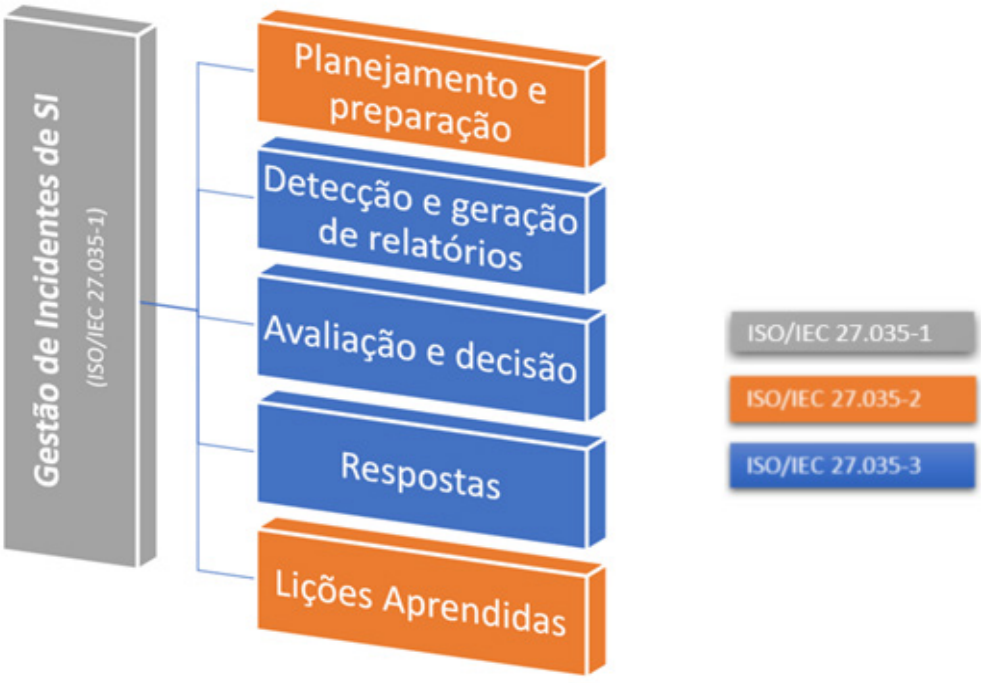

Figura 1 – Fases da norma ABNT ISO/IEC 27.035
(Gráfico produzido pela autora)

Em complemento à figura 1, a qual apresenta as três fases tratadas pela norma da ABNT ISO/IEC 27035-3, foi produzida a figura 2 para detalhar as operações de resposta a incidentes. Nela constam as operações para:

identificação de incidentes; avaliação e qualificação de incidentes; coleta de inteligência de ameaças; contenção, erradicação e recuperação de incidentes; análise de incidentes; e geração de relatórios de incidentes.

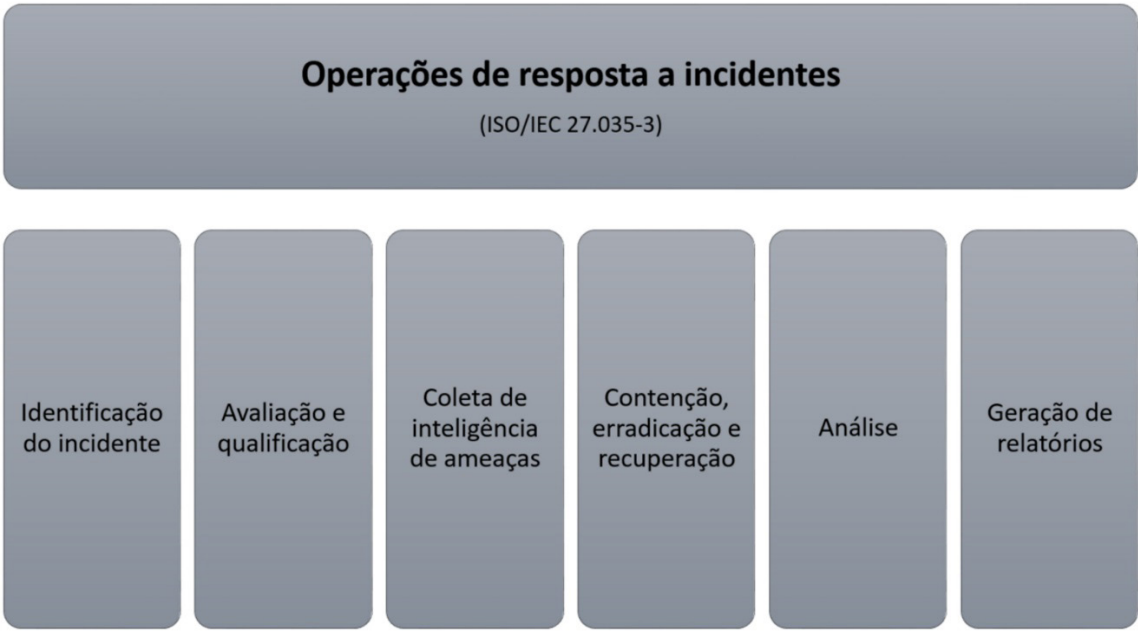

Figura 2 – Detalhamento da fase de operações segundo a norma ABNT ISO/IEC 27035-3

(Gráfico produzido pela autora)

Ao observar a legislação publicada pelo CNJ, nota-se que o Anexo I da Portaria 162 CNJ trata do Protocolo de Prevenção de Incidentes Cibernéticos do Poder Judiciário, o qual aborda as principais diretrizes necessárias para sua implantação. Esse protocolo é a base para o tratamento de incidentes cibernéticos. Quando se tratar de crise cibernética envolverá o Anexo II e, por fim, quando se tratar de investigação de ilícito cibernético envolverá o Anexo III.

O protocolo de prevenção é o início do tratamento de incidentes e ele é dividido nas seguintes fases:

- Preparação;
- Identificação;
- Contenção;
- Erradicação;
- Recuperação;
- Lições aprendidas.

Pode-se perceber as similaridades presentes no modelo proposto na legislação publicada pelo CNJ e a apresentada na série ISO/IEC 27.035.

Já o protocolo de gerenciamento de crise cibernética é acionado quando caracterizada uma crise, ou seja, quando o incidente apresentar pelo menos uma das seguintes características:

- Ficar caracterizado grave dano material ou de imagem;
- Restar evidente que as ações de resposta ao incidente cibernético provavelmente persistirão por longo período, podendo se estender por dias, semanas ou meses;
- Impactar a atividade finalística ou o serviço crítico mantido pela organização;
- Atrair grande atenção da mídia e da população em geral.

Esse protocolo é composto pelas seguintes fases:

- Planejamento da crise (pré-crise);
- Execução (durante a crise);
- Melhoria contínua (lições aprendidas no pós-crise).

Por fim, o protocolo de investigação para ilícitos cibernéticos é acionado quando identificar que o incidente é enquadrado como um crime cibernético e, consequentemente, penalmente relevante, e possui as seguintes fases:

- Coleta;
- Preservação;
- Comunicação.

Esses protocolos foram tratados individualmente na legislação, mas funcionam de maneira interligada conforme mostra a visão macro apresentada abaixo com base na Política de Segurança Cibernética (PSEC-PJ), a qual se encontra na Resolução CNJ 396, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ) e na interpretação analítica dos protocolos da Portaria CNJ 162.

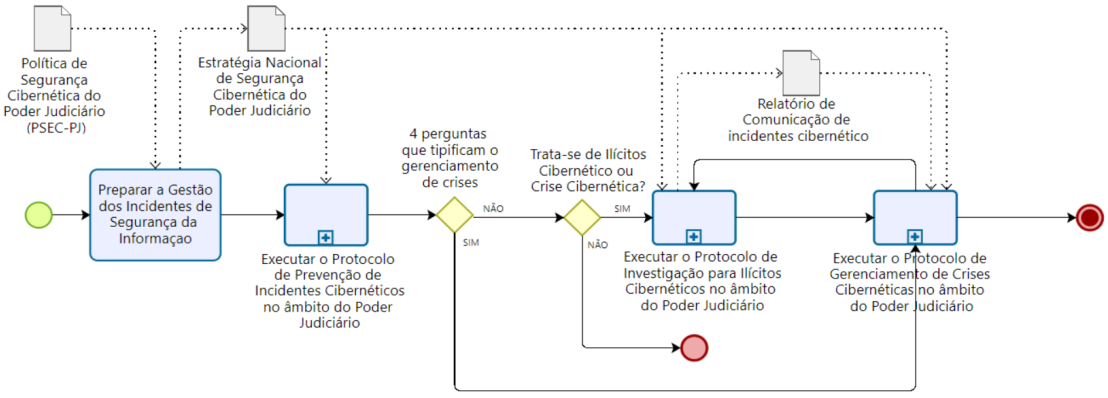

Figura 3 – Visão macro do fluxo de tratamento de incidentes de segurança da informação

(Gráfico produzido pela autora)

4 Crimes informáticos

No final da década de 1990, mediante contrato firmado entre a Comissão Europeia e a Universidade de Würzburg, representada pelo jurista alemão Ulrich Sieber, foi desenvolvido um estudo com o objetivo de fornecer à Comissão Europeia informações atualizadas sobre as questões jurídicas relativas a crimes relacionados a computadores, estabelecendo as ligações necessárias com o desenvolvimento da sociedade da informação (SIEBER, 1998).

Em seu estudo, Sieber (1998) menciona que a história dos crimes informáticos remonta à década de 1960, quando os primeiros artigos sobre casos dos chamados "crimes informáticos" foram publicados na imprensa pública e na literatura científica. Esses casos inicialmente incluíam manipulação, sabotagem e espionagem em computadores e o uso ilegal de sistemas de computadores. Já no meio da década de 1970, foi conduzido o primeiro estudo empírico sobre crime informático aplicando métodos científicos de pesquisa criminológica, o qual trouxe um número limitado de casos, mas ao mesmo tempo sugeriu um alto número estimado de casos não detectados ou não relatados de crimes informáticos.

Na década de 1980, Sieber (1998) cita como as visões sobre o assunto mudaram radicalmente, quando a imprensa publicou casos surpreendentes sobre *hackers*, vírus e *worms*. Além disso, a ampla onda de programas piratas, manipulação de caixas eletrônicos e abusos de telecomunicações revelaram a vulnerabilidade de uma sociedade da informação e também a necessidade de uma nova estratégia de segurança e controle do crime. Também se observou, nessa época, que os crimes não eram mais limitados a questões econômicas, mas também

incluíam ataques contra todos os tipos de interesses. Tudo isso favoreceu para que na década de 1990 a distribuição de conteúdo ilegal na internet fosse integrada ao conceito amplo estabelecido para crimes informáticos.

O termo "crimes informáticos" possui diferentes nomenclaturas a depender do autor, entre elas estão: crimes informáticos (SIEBER, 1998, p.19), delitos informáticos (VIANNA; MACHADO, 2013, p.19), ilícitos cibernéticos (CNJ, 2021a), crimes cibernéticos (WENDT; JORGE, 2013, p.18), tecnológicos, telemáticos, por computador, entre outros.

Sieber (1998) traz o conceito de "crime informático" definido por um grupo de *experts* da Organização para a Cooperação e Desenvolvimento Econômico (OECD), em 1983, do qual ele fazia parte. O termo foi definido como qualquer comportamento ilegal, antiético ou não autorizado, envolvendo processamento de dados automático e/ou transmissão de dados.

Para Vianna e Machado (2013), a denominação mais precisa é "crimes informáticos" ou "delitos informáticos", pois baseiam-se na inviolabilidade das informações automatizadas (dados), bem jurídico penalmente tutelado.

Já para Wendt e Jorge (2013), o termo "crimes cibernéticos" define os delitos praticados contra ou por intermédio de computadores (dispositivos informáticos, em geral).

Como as legislações utilizam termos diferentes para referir-se a "crimes informáticos", no decorrer deste artigo será utilizado o termo que melhor se adequar a citação no momento.

No Brasil, a tipificação de crimes informáticos é esparsa, mas começou a ser tratada nas Leis 12.735/2012 e 12.737/2012. Em seguida, foi promulgado o Marco Civil da Internet, Lei 12.965/2014, a qual foi alterada pela Lei Geral de Proteção de Dados Pessoais (LGPD), Lei 13.853/2019. Devido ao aumento nos casos envolvendo esse tipo de crime, a Lei 14.155, de 27 de maio de 2021, foi sancionada, e torna mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet.

Nos subtítulos abaixo serão abordadas as tipologias dos crimes informáticos e sua tipificação na legislação brasileira.

4.1 Tipologias

A respeito das tipologias existentes de crimes informáticos, existem algumas correntes que serão citadas a seguir.

Em seu livro sobre prova digital no processo penal, Kist (2019) define que a tipologia dos crimes informáticos pode ser visualizada em sentido amplo ou estrito. O primeiro envolve todas as atividades criminosas executadas por meio informático, sendo direcionada ao ambiente cibernético ou utilizando ele como instrumento para praticar crimes comuns. Já o sentido estrito defende que crimes informáticos abarcam somente os crimes onde o elemento digital seja o objeto de proteção principal (KIST, 2019).

Por outro lado, Vianna e Machado (2013) classificam os crimes informáticos em crimes informáticos impróprios, próprios, mistos e mediatos ou indiretos. Para os autores, os próprios são crimes na qual o bem protegido é a inviolabilidade das informações armazenadas ou em trânsito, como a invasão de dispositivo informático e a inserção de dados falsos em sistema por funcionário público, tipificado no art. 313-A do Código Penal. Por sua vez, os impróprios envolvem dispositivos informáticos sendo utilizados como mero instrumento para execução de um crime, não ofendendo a inviolabilidade da informação automatizada, como em crimes de ameaça, art. 147 do Código Penal, por meio de correio eletrônico ou rede social. Já os crimes informáticos mistos são complexos, pois além de tratar a proteção da inviolabilidade, também tutela o bem jurídico de natureza diversa, cenário presente no crime de acesso ao sistema do serviço eleitoral com o intuito de alterar a apuração ou contagem de votos, art. 72, inciso I, Lei 9.504/1997. Por último, os mediatos ou indiretos, os quais são caracterizados como atividade-fim não informática herdando o aspecto da atividade-meio, informatizada, para proporcionar sua execução. Como exemplo, pode-se citar a invasão de um sistema de um banco e transferência ilegal de recursos financeiros. Nesse caso, a invasão de dispositivo informático é o primeiro crime (delito informático) e o furto é o segundo (delito contra o patrimônio), mas o agente somente seria punido pelo furto devido ao princípio da consunção.

Outra perspectiva, como mostra PAULINO; SCHOUCAIR; JUNIOR; MAIA (2021), mais difundida, ao menos no Brasil, é a classificação apenas de crimes próprios ou impróprios. Crimes digitais próprios ou puros ocorrem

quando há o uso do computador como fim, ou seja, alvo. Exemplos: invadir dispositivo informático, *cyberbulling*, impulsionamento de conteúdo no dia das eleições, pirataria, etc. Já nos impróprios ou impuros, o computador é usado como meio. Exemplos: estelionato e outras fraudes, pornografia infantil, crimes contra a honra, crime contra o sistema financeiro e lavagem de dinheiro, furto, dano, ameaça, etc.

4.2 Tipificação dos crimes informáticos

No Brasil não existe uma lei única que trata a tipificação dos cibercrimes, logo, um conjunto de leis caracterizam, dentro do seu escopo, as condutas informáticas que podem ser evidenciadas por uma ou mais técnicas ou artefatos. Comportamentos recorrentes ou intoleráveis na sociedade tiveram relevância penal no cenário brasileiro e deram origem às Leis 12.735/2012 e 12.737/2012. Jesus e Milagre (2016) citam em seu livro algumas condutas que podem caracterizar crime. São elas:

- acesso ilegítimo (Código Penal, art. 154-A);
- interceptação ilegítima (Lei 9.296/1996, art. 10);
- interferência de dados/dano informático (se invadir e causar dano [Código Penal, art. 154-B], se apenas causar dano [Código Penal, art. 163]);
- interferência em sistemas (Código Penal, art. 266);
- uso abusivo de dispositivos (Código Penal, art. 154-A e 325);
- falsidade ou fraude informática (Código Penal, art. 299, 313-A e 313-B);
- burla informática/sabotagem informática (não há tipo penal claro no Brasil);
- furto de dados ou vazamento de informações (Lei 9.279/1996 e Código Penal, art. 153);
- pichação informática ou *defacement* (Código Penal, art. 154-A, por pressupor invasão);
- envio de mensagens não solicitadas/*spam* (não há tipo penal claro no Brasil);
- uso indevido informático (não há tipo penal claro no Brasil).

Seguem outras legislações que podem caracterizar ilícitos: Lei 9.504/1997, art. 72, I a III (normas para as eleições – acesso a sistema para alterar a apuração ou a contagem de votos; introduzir comando, instrução, ou programa de computador capaz de destruir, apagar, eliminar, alterar, gravar ou transmitir dado; causar, propositadamente, dano físico ao equipamento); Lei 8.069/1990, arts. 241, 241-A a 241-D (Estatuto da Criança e do Adolescente – casos que envolvam criança ou adolescente em atividades sexuais explícitas, reais ou simuladas, ou exibição dos órgãos genitais de uma criança ou adolescente para fins primordialmente libidinosos); Lei 7.716/1989, art. 20 (crimes resultantes de preconceito de raça ou de cor); Lei 9.609/1998, art. 12 (violação dos direitos de autor de programa de computador); Decreto-Lei 2.848/1940, Código Penal, art. 138 (calúnia), art. 139 (difamação) e art. 140 (injúria), art. 147 (ameaça), art. 171 (estelionato), art. 286 (incitação ao crime) e art. 287 (apologia de crime ou criminoso).

É importante mencionar tipos de evidências que podem ser encontradas e caracterizar os crimes citados acima, mas, antes, deve-se conhecer o princípio ou teoria de Locard, o qual foi criado pelo cientista, pioneiro da ciência forense, Edmond Locard, e seu conceito explanado no livro de Araújo, Monteiro; Martins (2018). A teoria diz que "a base da investigação de um crime é identificar vestígios que apontem o autor do crime, que demonstre o crime em si e a ligação do criminoso com o crime e com a vítima" (ARAÚJO, MONTEIRO; MARTINS, 2018, p. 22 e 23). Araújo, Monteiro; Martins (2018) mencionam em seu livro que, para o professor Edmond Locard, cada contato deixará uma marca/rastro, logo, quando aplicado esse pensamento a crimes cibernéticos, pode-se entender que essas marcas seriam as evidências encontradas no processo de investigação, por isso a importância da preservação e coleta, pois se uma das etapas não for feita adequadamente, pode afetar a integridade das provas ou até mesmo gerar injustiças.

As condutas consideradas crimes informáticos podem ser praticadas por meio de artefatos, técnicas ou métodos. Jesus e Milagre (2016) apresentam as mais comuns: vírus[3], *trojan*[4], *sniffer*[5], *backdoor*[6], *spyware*[7], *rootkits*[8], DoS e DDoS[9], DNS *poisoning*[10], *brute force*[11], *defacement*[12], entre outros. Atualmente, o que está mais presente na mídia são os ataques envolvendo *ransomware*[13], o qual pode envolver vários crimes como extorsão, vazamento de informações e interrupção de serviço informático.

4.3 Evidência digital

Há quatro conceitos importantes em uma investigação digital. São eles: vestígio, evidência, prova e indício. É por meio deles que se define a materialidade dos fatos e a existência de indícios de autoria dos delitos.

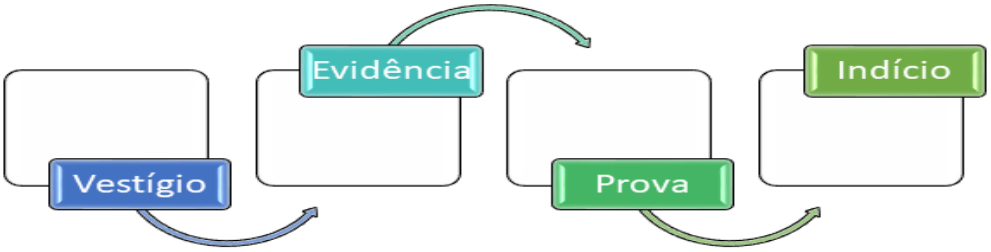

Figura 4 – Sequência de conceitos
(Gráfico produzido pela autora)

[3] É uma "seção oculta e autorreplicante de um *software* de computador, geralmente utilizando lógica maliciosa, que se propaga pela infecção (inserindo uma cópia sua e tornando-se parte) de outro programa. Não é auto executável, ou seja, necessita que o seu programa hospedeiro seja executado para se tornar ativo" (PRESIDÊNCIA DA REPÚBLICA, 2021).

[4] Também conhecido como cavalo de Tróia, é um "tipo de *malware* que, além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário" (PRESIDÊNCIA DA REPÚBLICA, 2021).

[5] Um *sniffer* é um aplicativo ou dispositivo que pode ler, monitorar e capturar trocas de dados de rede e ler pacotes de rede. Se os pacotes não estiverem criptografados, um *sniffer* fornecerá uma visão completa dos dados dentro do pacote (MICROSOFT, 2022).

[6] É "qualquer mecanismo inserido no sistema, intencionalmente ou acidentalmente, com o objetivo de permitir o acesso não documentado ao sistema ou aos seus dados" (PRESIDÊNCIA DA REPÚBLICA, 2021).

[7] Também conhecido como programa espião, ele é um "tipo de *malware*. Programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros. *Keylogger, screenlogger* e *adware* são alguns tipos específicos de *spyware*" (PRESIDÊNCIA DA REPÚBLICA, 2021).

[8] O *rootkit* é um "conjunto de programas e de técnicas que permitem esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido. É importante ressaltar que o nome *rootkit* não indica que as ferramentas que o compõem são usadas para obter acesso privilegiado em um computador (*root* ou *administrator*), mas, sim, para manter o acesso privilegiado em um computador previamente comprometido" (PRESIDÊNCIA DA REPÚBLICA, 2021).

[9] "Negação de serviço, ou DoS (*Denial of Service*), é uma técnica pela qual um atacante utiliza um computador para tirar de operação um serviço, um computador ou uma rede conectada à Internet. Quando utilizada de forma coordenada e distribuída, ou seja, quando um conjunto de computadores é utilizado no ataque, recebe o nome de negação de serviço distribuído, ou DDoS (*Distributed Denial of Service*)" (CERT.br, 2012, p. 21).

[10] É conhecido como envenenamento do cache de DNS (PRESIDÊNCIA DA REPÚBLICA, 2021).

[11] "Um ataque de força bruta, ou *brute force*, consiste em adivinhar, por tentativa e erro, um nome de usuário e senha e, assim, executar processos e acessar sites, computadores e serviços em nome e com os mesmos privilégios deste usuário." (CERT.br, 2012, p. 20).

[12] "Desfiguração de página, *defacement* ou pichação, é uma técnica que consiste em alterar o conteúdo da página Web de um site." (CERT.br, 2012, p. 21).

[13] É um tipo de *malware,* que, por meio de criptografia, impede o acesso a dados computacionais. Para recuperar o acesso, exige-se pagamento de um valor de resgate. Caso o pagamento do resgate não seja realizado, pode-se perder definitivamente o acesso aos dados sequestrados (PRESIDÊNCIA DA REPÚBLICA, 2021).

No Código de Processo Penal (CPP), art. 158-A, § 3º, o vestígio é caracterizado como "todo objeto ou material bruto, visível ou latente, constatado ou recolhido, que se relaciona à infração penal", ou seja, é o material bruto que o perito coleta em um exame pericial qualquer e que possa ter relação com o fato investigado.

Os vestígios que podem servir como elemento de prova segundo Araújo, Monteiro e Martins (2018) são: dados voláteis, dados transitórios, dados não voláteis e dados frágeis. Os dados voláteis estão presentes na memória principal (RAM) do computador, logo, só estarão armazenados enquanto houver energia elétrica e podem ser modificados, como usuários logados, conexões de rede, processos, área de transferência, entre outros. Após o desligamento do computador esses dados são perdidos e não mais será possível realizar sua coleta. Já os dados transitórios são como os voláteis, mas de curtíssima duração, pois enquanto o computador está ligado, dados podem ser apagados/sobrepostos. Normalmente reside na memória *cache* e possui informações como usuários que fizeram *logout*, informações de abertura de conexão de rede. Também existem os dados não voláteis, os quais encontram-se na memória secundária (HD, SSD, CD, DVD, *pendrive*), que possui como objeto de investigação arquivos em geral, *swap*, registros, eventos e *logs*. A análise desses dados deve ser feita protegida de escrita. Por fim, os dados frágeis, eles também se encontram na memória secundária, contudo, são temporários e podem ser modificados, tal como último acesso, modificação ou impressão, acesso de arquivos, entre outros.

Após a análise do vestígio digital, caso esse seja comprovadamente relacionado ao fato investigado, ele será denominado evidência digital. Segundo definição do dicionário Priberam (2021), evidência é uma certeza manifesta, é algo que serve para demonstrar ou esclarecer um fato, uma verdade ou uma causa.

Aprofundando um pouco sobre o tema, a norma técnica da ABNT ISO/IEC 27037 (2013) apresenta os três princípios fundamentais que governam a evidência digital: relevância (possui informação de valor para investigação), confiabilidade (é passível de auditoria e justificação) e suficiência (material recolhido foi suficiente para executar corretamente a investigação).

Por sua vez, a prova digital é a formalização da evidência digital como parte do conjunto probatório no contexto do processo. A prova pode ser classificada como informativa (depoimentos de testemunhas, autor, vítimas), material (vestígios produzidos ou decorrentes de conduta), complementar (elementos ou dados auxiliares que reforçam/confirmam as demais provas) ou circunstancial (algo conhecido e provado, que tem relação com o fato, autorizando, por indução, concluir a existência de outras circunstâncias) (ARAÚJO; MONTEIRO; MARTINS, 2018).

Por fim, o indício, o qual é definido no art. 239 do CPP como "a circunstância conhecida e provada, que, tendo relação com o fato, autorize, por indução, concluir-se a existência de outra ou outras circunstâncias".

Como o foco deste artigo são as fases de tratamento em caso de incidente cibernético envolvendo ilícito penal, ou seja, crime, os termos "vestígio" e "evidência" são os mais importantes para os órgãos da Justiça Federal dentro das ações que serão responsáveis no processo. Apesar das diferenças conceituais entre os termos citados, aqueles serão tratados como sinônimos.

5 Computação forense aplicada à prática criminosa

A computação forense está ganhando um espaço de destaque nas organizações, nas polícias e na sociedade de modo geral. Com o aumento na quantidade de crimes informáticos, a computação forense traz a possibilidade de identificar ataques, melhorar as formas de defesa do ambiente, revelar os fatos e punir os autores de delitos.

Segundo Velho (2016), "computação forense é a ramificação da Criminalística que tem como objetivo a análise de vestígios cibernéticos, englobando os elementos que os orbitam". Para ele, essa análise de vestígios permite a elucidação de delitos, os quais envolvem três fatores: materialidade (mostra claramente que um fato aconteceu ou não), autoria (descoberta da pessoa que cometeu o delito) e motivação (o que levou o autor a praticar a ação).

Apesar dos cuidados a fatores que podem impactar os exames periciais, humano, tecnológico e legal, é importante observá-los para que não viole a integridade das provas. Além da aplicação de métodos científicos,

também é utilizado o documento chamado "Termo de Custódia[14]", o qual permite o acompanhamento da movimentação das evidências, e nele constará cada indivíduo que manuseou a evidência, o momento da coleta e/ou transferência e o propósito dela.

A computação forense possui algumas aplicações práticas, entre elas: fins legais (apuração de crimes e contravenções), disciplinares corporativos (investigação do uso indevido de recursos e serviços de uma instituição; aplicação de legislações e normas como a LGPD, a Política de Segurança da Informação, etc.) e pessoais (auxiliar na recuperação de dados e informações, controle parental).

Contudo, Pinheiro (2021) descreve em sua obra que para a correta aplicação da computação forense são utilizados métodos científicos para preservação, coleta, validação, identificação, análise, interpretação, documentação e apresentação de evidências digitais com validade probatória em juízo.

Portanto, com as ciências forenses é possível descobrir seis elementos: materialidade (o que aconteceu), autoria (quem), dinâmica (como), temporalidade (quando), local (onde) e motivação (porque), e assim, elucidar práticas criminosas.

6 Crise cibernética x investigação de ilícito

Após entender os conceitos básicos que permeiam a segurança cibernética, a gestão em caso de incidentes de segurança da informação e tipificação de delitos informáticos, pode-se iniciar o detalhamento do Protocolo de Investigação para Ilícitos Cibernéticos (PIILC), o qual encontra-se no Anexo III da Portaria CNJ 162 de 10 de junho de 2021. Esse protocolo "tem por finalidade estabelecer os procedimentos básicos para coleta e preservação de evidências e para comunicação obrigatória dos fatos penalmente relevantes ao Ministério Público e ao órgão de polícia judiciária com atribuição para o início da persecução penal" (CNJ, 2021a).

Há dois casos em que o PIILC será acionado: quando o incidente for classificado como penalmente relevante e/ou quando for classificado como crise cibernética. Isso ocorre devido à interseção entre os dois protocolos, ou seja, um fará parte do outro em algum ponto.

A crise cibernética será iniciada nos seguintes casos, conforme protocolo: caso caracterize grave dano material ou de imagem; caso as ações de resposta persistirem por longo período; caso impacte a atividade finalística ou o serviço crítico mantido pela organização; ou caso atraia grande atenção da mídia e da população em geral.

A responsabilidade de coordenação da crise é do Comitê de Crise Cibernética – CCC e entre suas atribuições está a aplicação do Protocolo de Investigação para Ilícitos Cibernéticos do Poder Judiciário (PIILC). Esse protocolo propiciará a coleta das evidências e sua preservação, além da comunicação ao Ministério Público e Polícia Judiciária, durante a crise cibernética. Após seguir esse fluxo, deve-se retornar ao Protocolo de Gerenciamento de Crises Cibernéticas (PGCRC) para tratar internamente o incidente.

7 Fluxo da investigação de ilícito cibernético

Quando se pensa em uma investigação de crime informático ou ilícito cibernético, é importante entender a anatomia geral de um ataque cibernético. Jesus e Milagre (2016) entendem que os passos descritos na imagem abaixo são os principais.

[14] Documento para registro e controle da cadeia de custódia, a qual é um "processo que acompanha o movimento de evidência, por meio de sua coleta, salvaguarda e ciclo de análise, documentando cada indivíduo que manuseou a evidência, o momento (data e hora) em que a evidência foi coletada ou transferida e o propósito de cada transferência. Contribui para a validação da prova pericial e do respectivo laudo gerado, porque garante a idoneidade e rastreabilidade dos vestígios, com a finalidade de preservar a confiabilidade e transparência até que o processo seja concluído" (PRESIDÊNCIA DA REPÚBLICA, 2021).

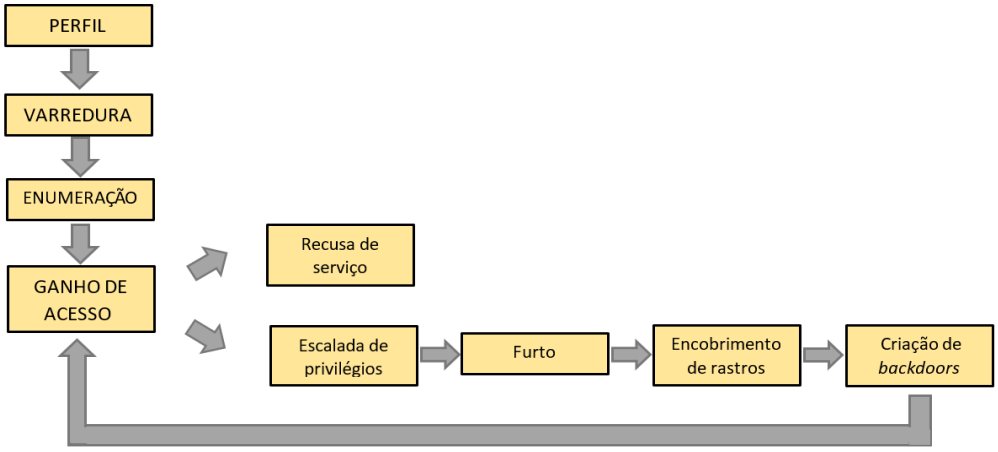

Figura 5 – Anatomia genérica de ataques cibernéticos

Fonte: adaptado de Jesus (2016).

Para eles, as três primeiras fases, "perfil", "varredura" e "enumeração" não são atos puníveis por serem apenas atos preparatórios, mero reconhecimento do ambiente. A partir da fase de "ganho de acesso" o ataque passa a ganhar relevância criminal de acordo com o art. 154-A do Código Penal, que tipifica a invasão (BRASIL, 1940).

Ao identificar alguma ação suspeita, como a citada acima, deve-se comunicar a Equipe de Tratamento e Resposta a Incidentes (ETIR), a qual iniciará o processo de tratamento. Após uma análise e categorização, caso identificado como um ilícito cibernético, o órgão do Poder Judiciário deve iniciar o Protocolo de Investigação de Ilícito Cibernético (PIILC), o qual possui as seguintes fases:

- Coleta;
- Preservação;
- Comunicação.

Após a execução dessas fases, outro protocolo é acionado, o Protocolo de Gerenciamento de Crise Cibernética (PGCC), o qual dará prosseguimento aos tratamentos internos ao órgão que tem objetivos distintos aos do Ministério Público e Polícia Judiciária.

Com o intuito de auxiliar os órgãos, o protocolo explicita alguns pré-requisitos para adequação dos ativos de tecnologia da informação, os quais possibilitarão a coleta de evidências futuras. Entre eles estão: sincronização de ativos com a Hora Legal Brasileira (HLB) e registro de eventos (*logs*).

Para um melhor entendimento, foi criado o fluxo abaixo com as tarefas de cada uma dessas fases.

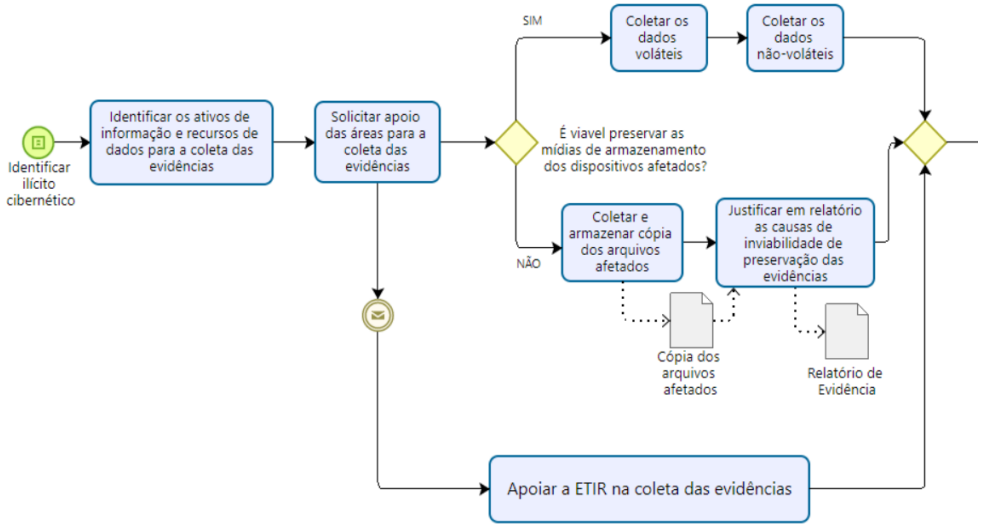

Figura 6 – Fase de coleta de evidências

(Gráfico produzido pela autora)

Ao identificar o ilícito cibernético, deve-se definir o local do crime e, partir desse ponto, iniciar a identificação dos ativos envolvidos, seus responsáveis e a amplitude da ameaça em questão, para assim definir o escopo para coleta de evidências. O procedimento de coleta, seja físico e/ou lógico, deverá seguir os critérios mínimos para não interferir na integridade dos dados, e entre os passos está o isolamento dos ativos. A coleta deve iniciar pelos dados voláteis, quando possível, e depois os dados não voláteis. Caso houver algum impeditivo ou complicação na coleta, isso deve ser justificado em relatório, além de coletar e armazenar uma cópia dos arquivos afetados pelo incidente: "*logs*, configurações do sistema operacional, arquivos do sistema de informação, e outros julgados necessários, mantendo-se a estrutura de diretórios original e os 'metadados' desses arquivos, como data, hora de criação e permissões" (CNJ, 2021a).

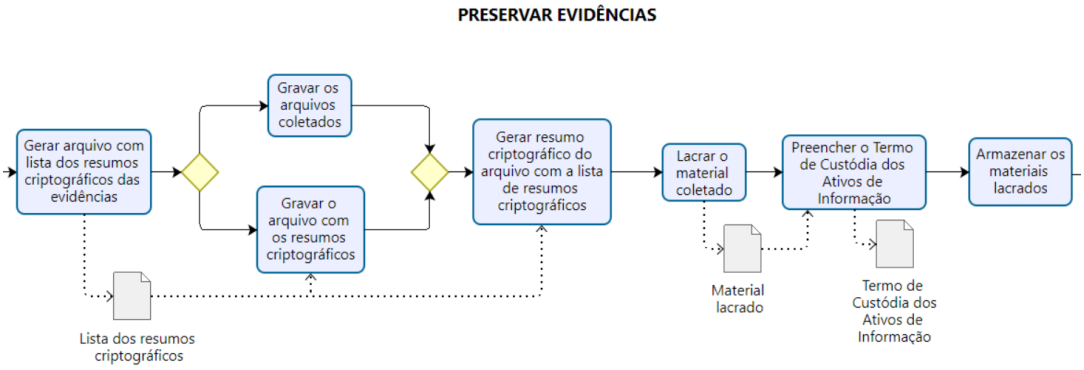

Figura 7 – Fase de preservação das evidências

(Gráfico produzido pela autora)

Após a conclusão da fase de coleta, inicia-se a fase de preservação das evidências. O protocolo descreve que primeiramente deve-se gerar o resumo criptográfico (*hash*) de cada uma das evidências coletadas e armazenar em um arquivo. Deve-se, em seguida, gerar o *hash* desse arquivo com os *hashs*. Os arquivos coletados (originais/cópia forenses) serão lacrados e armazenados em local restrito e controlado, após o preenchimento do "Termo de Custódia".

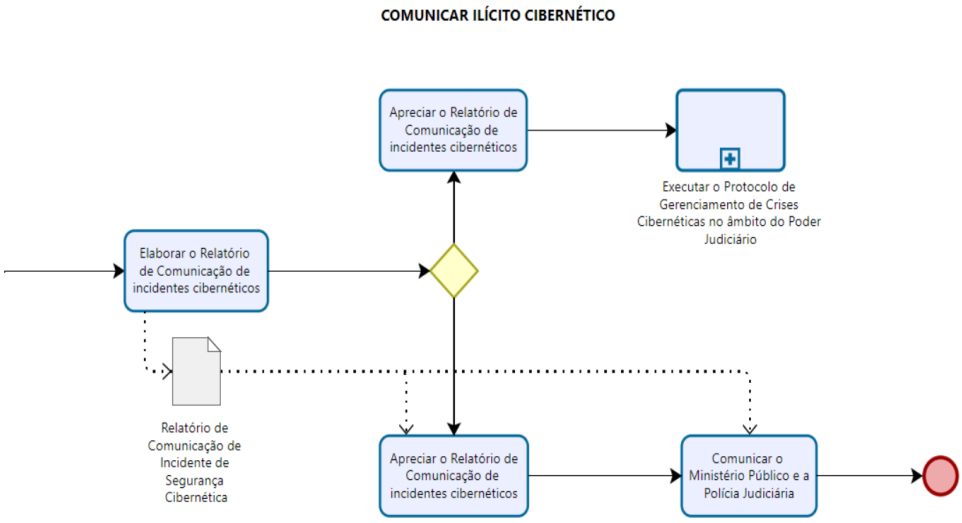

Figura 8 – Fase de comunicação de ilícito cibernético

(Gráfico produzido pela autora)

Por fim, a fase de comunicação do ilícito cibernético. Ela inicia com a elaboração do relatório de comunicação de incidentes cibernéticos. Segundo o protocolo em questão, o relatório deve conter no mínimo as seguintes informações:

1. Nome do responsável pela preservação dos dados do incidente, com informações de contato;
2. Nome do agente responsável pela ETIR e informações de contato;
3. Órgão comunicante com sua localização e informações de contato;
4. Número de controle da ocorrência;
5. Relato sobre o incidente que descreva o que ocorreu, como foi detectado e quais dados foram coletados e preservados;
6. Descrição das atividades de tratamento e resposta ao incidente e todas as providências tomadas pela ETIR, incluindo as ações de preservação e coleta, a metodologia e as ferramentas utilizadas e o local de armazenamento das informações preservadas;
7. Resumo criptográfico dos arquivos coletados;
8. Termo de Custódia dos Ativos de Informação Relacionados ao Incidente de Segurança;
9. Número de lacre de material físico preservado, se houver; e
10. Justificativa sobre a eventual inviabilidade de preservação das mídias de armazenamento dos dispositivos afetados, diante da impossibilidade de mantê-las.

Após preenchimento do relatório, ele deve ser colocado em um envelope lacrado e rubricado pelo agente responsável pela ETIR, constando apenas a informação de que se trata de comunicação de evento relacionado à segurança da informação, e, por fim, protocolado e encaminhado formalmente à autoridade responsável pelo órgão do Poder Judiciário afetado. Essa autoridade é quem encaminhará formalmente ao Ministério Público e ao órgão de polícia judiciária para apuração dos fatos.

Embora a apuração seja realizada pela polícia judiciária, o órgão ainda necessita tratar o incidente internamente, a fim de resolver os problemas causados e evitar problemas futuros. Por esse motivo, no fluxo está previsto a execução do Protocolo de Gerenciamento de Crise Cibernética, o qual detém essa função.

Entre as atividades que devem ser executadas no Protocolo de Gerenciamento de Crise Cibernética, estão:

- Solicitar a colaboração de especialistas ou de centros de resposta a incidentes de segurança, caso necessário;

- Avaliar necessidade de recursos adicionais extraordinários;
- Orientar sobre as prioridades e estratégias da organização para recuperação;
- Definir os procedimentos de compartilhamento de informações relevantes com outros órgãos;
- Elaborar e executar o plano de retorno à normalidade;
- Analisar as ações do incidente de segurança e identificar as lições aprendidas;
- Elaborar o relatório de encerramento do incidente de segurança;
- Encerrar o tratamento do incidente.

Portanto, pode-se afirmar que após a execução dos protocolos descritos, o incidente de segurança envolvendo ilícito cibernético terá sido tratado internamente e encaminhado para os órgãos externos competentes investigarem.

8 Considerações finais

A fim de propiciar o melhor entendimento possível sobre o tema, foi necessário apresentar diversos conceitos, como o de segurança cibernética, crimes informáticos, gestão de incidentes, entre outros.

Neste artigo, o objetivo era tratar de forma sequencial os temas importantes para a explicação do fluxo presente nos protocolos publicados pelos órgãos de justiça, mas principalmente o Protocolo de Investigação de Ilícito Cibernético (PIILC).

Entende-se que os protocolos detêm as diretrizes para que os órgãos do Poder Judiciário possam iniciar o tratamento de incidentes de segurança da informação e, consequentemente, melhorar seu nível de maturidade no assunto. Logo, a primeira iniciativa foi executada, devendo cada órgão discutir a questão visando implantar tais diretrizes internamente o mais breve possível, haja visto o cenário de ataques cibernéticos cada vez mais frequentes.

Por fim, é importante frisar a abrangência do tema "segurança cibernética" e as aplicações da computação forense. Este artigo destaca a gestão do processo, mas há outros aspectos que podem ser aprofundados, como as técnicas e as ferramentas utilizadas em uma perícia digital.

9 Referências

ABNT, ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27001. Tecnologia da informação: técnicas de segurança: sistemas de gestão da segurança da informação: requisitos. Rio de Janeiro: ABNT, 2013.

ABNT, ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27002. Tecnologia da informação: técnicas de segurança: código de prática para controles de segurança da informação. Rio de Janeiro: ABNT, 2013.

ABNT, ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27035-3. Tecnologia da informação: Gestão de incidentes de segurança da informação, parte 3: diretrizes para operações de resposta a incidentes de TIC. Rio de Janeiro: ABNT, 2021.

ABNT, ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27037. Tecnologia da informação: técnicas de segurança: diretrizes para identificação, coleta, aquisição e preservação de evidência digital. Rio de Janeiro: ABNT, 2013.

AC CERTIFICAMINAS. Crescimento de crimes cibernéticos na pandemia: como não ser uma vítima. *Crypto ID*, abr. 2021. Disponível em: https://cryptoid.com.br/identidade-digital-destaques/crescimento-de-crimes-ciberneticos-na-pandemia-como-nao-ser-uma-vitima/. Acesso em: 30 out. 2021.

ARAÚJO, Antonio; MONTEIRO, Marcos; MARTINS, Luiz Antonio. *Informática forense*. São Paulo: Leud, 2018. v. 2.

BRASIL. *Decreto-lei nº 2.848, de 7 de dezembro de 1940*. Código penal. Brasília: Presidência da República, [2022]. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 6 jun. 2022.

CASTELLS, Manuel. *A sociedade em rede*. São Paulo: Paz e Terra, 1999.

CERT.br – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. *Cartilha de segurança para Internet*. São Paulo: Comitê Gestor da Internet no Brasil, 2012.

CONSELHO DA JUSTIÇA FEDERAL (CJF). *Portaria nº 68 CJF, de 10 de fevereiro de 2021*. Dispõe sobre a aprovação do Plano de Ação de Segurança Cibernética na Justiça Federal, de que tratam as Resoluções CNJ n. 360, n. 361 e n. 362, de 17 de dezembro de 2020. Disponível em: https://www.in.gov.br/web/dou/-/portaria-n-68-cjf-de-10-de-fevereiro-de-2021-303776132. Acesso em: 24 out. 2021.

CONSELHO DA JUSTIÇA FEDERAL (CJF). *Resolução nº 687 CJF, de 15 de dezembro de 2020*. Dispõe sobre a alteração da Resolução CJF n. 6, de 7 de abril de 2008. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-n-687-de-15-de-dezembro-de-2020-294641502. Acesso em: 24 out. 2021.

CONSELHO NACIONAL DE JUSTIÇA (CNJ). *Portaria nº 162 CNJ, de 10 de junho de 2021a*. Aprova protocolos e manuais criados pela Resolução CNJ nº 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ). Disponível em: https://atos.cnj.jus.br/atos/detalhar/3982. Acesso em: 24 out. 2021.

CONSELHO NACIONAL DE JUSTIÇA (CNJ). *Resolução nº 396 CNJ, de 07 de junho de 2021b.* Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ). Disponível em: https://atos.cnj.jus.br/atos/detalhar/3975. Acesso em: 24 out. 2021.

EVIDÊNCIA. *In:* DICIONÁRIO Priberam da língua portuguesa. Disponível em: https://dicionario.priberam.org/chave. Acesso em: 7 nov. 2021.

ISO, International Organization for Standardization. *ISO/IEC 27000*. Information technology: security techniques: information security management systems: overview and vocabulary. Switzerland: ISO, 2018.

JESUS, Damásio de; MILAGRE, José Antônio. *Manual de crimes informáticos*. São Paulo: Saraiva, 2016.

KIST, Dario José. *Prova digital no processo penal*. São Paulo: JH Mizuno, 2019.

MICROSOFT. *Common types of network attacks*. Redmond: Microsoft, 2012. Disponível em: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc959354(v=technet.10)?redirectedfrom=MSDN. Acesso em: 5 jun. 2022.

PAULINO, Galtiênio da Cruz; SCHOUCAIR, João Paulo Santos; JUNIOR, Octahydes Ballan; MAIA, Tiago Dias (org.). *Técnicas avançadas de investigação*: perspectivas prática e jurisprudencial. Brasília: ESMPU, 2021. v.1. p. 259-330.

PINHEIRO, Patrícia Peck. *Direito digital*. 7. ed. São Paulo: Saraiva, 2021.

PRESIDÊNCIA DA REPÚBLICA. Gabinete de Segurança Institucional. *Portaria GSI/PR nº 93, de 18 de outubro de 2021*. Aprova o glossário de segurança da informação. Brasília: Presidência da República: 2021. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-gsi/pr-n-93-de-18-de-outubro-de-2021-353056370. Acesso em: 24 out. 2021.

ROLFINI, Fabiana. Cibercrime: ataques no Brasil aumentam mais de 300% com a pandemia. *Olhar Digital*. São Paulo, jul. 2020. Disponível em: https://olhardigital.com.br/2020/07/03/seguranca/cibercrime-ataques-no-brasil-aumentam-mais-de-300-com-a-pandemia/. Acesso em: 30 out. 2021.

SECOM TCU. *Avaliação do TCU aponta que ataques cibernéticos merecem atenção governamental*. Brasília: TCU, 2020. Disponível em: https://portal.tcu.gov.br/imprensa/noticias/avaliacao-do-tcu-aponta-que-ataques-ciberneticos-merecem-atencao-governamental.htm. Acesso em: 30 out. 2021.

SIEBER, Ulrich. Legal *Aspects of computer-related crime in the information society:* COMCRIME study. Würzburg: University of Würzburg, 1998.

VELHO, Jesus Antonio. *Tratado de computação forense*. São Paulo: Millennium, 2016.

VIANNA, Túlio; MACHADO, Felipe. *Crimes informáticos conforme a Lei nº 12.373/2012*. Belo Horizonte: Fórum, 2013.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. *Crimes cibernéticos*: ameaças e procedimentos de investigação. Rio de Janeiro: Brasport, 2013.