Forensic readiness
Uma abordagem proativa de apoio à análise forense digital

Ana Carmen Collodetti Brügger [a,d*], Evandro Mário Lorens [c,b,d,a]

[a] IPOG, Brasília, DF, BRASIL, 70850-090

[b] UNB, Brasília, DF, BRASIL, 70910-900

[c] Polícia Federal, Brasília, DF, Brasil, 70610-902

Academia Brasileira de Ciências Forenses (ABCF), Brasília, DF, Brasil,

*e-mail: anaccbrugger@gmail.com

Resumo

As comunidades forenses e de segurança da informação identificam um número crescente de ações criminosas originadas dentro das empresas, tanto por ataques cibernéticos às informações causando enormes prejuízos monetários, quanto também às imagens das organizações. Em muitos casos, tais crimes não chegam aos tribunais para as devidas ações legais por ineficiência das próprias organizações em produzirem evidências digitais não refutáveis, sob o ponto de vista jurídico. Nesse contexto, considerando-se a irreversível dependência tecnológica das empresas e a necessidade de se prepararem para processos judiciais que podem surgir em decorrência de perícias digitais realizadas após a ocorrência de eventos considerados criminosos, nasce a ideia de se criar mecanismos que possam dar suporte à produção de provas digitais pelas organizações, de forma metódica e aderente às legislações a que se sujeitam. Forensic Readiness é um conceito introduzido por Tan (2001), visando preparar as organizações para futuros processos judiciais, que impliquem na apresentação de provas digitais. Neste trabalho buscou-se apresentar esse conceito sob diversas abordagens, a fim de demonstrar o estado atual das pesquisas, bem como sua abrangência e correlação com outras áreas de conhecimento. Na conclusão, apontam-se benefícios de sua adoção e linhas de pesquisa que podem ser derivadas desse conceito.

Palavras-chave: Análise forense digital. Digital forensic readiness. Forensic readiness. Governança. Perícia digital.

1 - Introdução

A análise forense digital (AFD) trata da aplicação do conhecimento científico combinado com elementos legais para coletar e analisar dados de sistemas de computadores, redes, comunicações e dispositivos de armazenamento, de forma metódica, para que essas informações sejam preservadas e, posteriormente, admissíveis como provas em um tribunal (US-CERT, 2008).

Geralmente, nas organizações, a AFD faz parte da aptidão para responder aos incidentes de segurança (FREILING e SCHWITTAY, 2007). Enquanto o principal objetivo da resposta aos incidentes (RI) é restaurar os serviços computacionais o mais rápido possível e aprender sobre um incidente de segurança, a AFD dá ênfase especial ao tratamento correto de possíveis vestígios digitais, que podem ser usados como provas no tribunal, para evitar de serem alterados ou adulterados (FREILING; SCHWITTAY, 2007).

Embora haja convergência técnica e operacional entre as disciplinas RI e AFD, ambas investiguem incidentes digitais, utilizem, em várias situações, as mesmas ferramentas e métodos, e compartilhem as principais fases do processo investigativo, há diferenças significativas nos resultados produzidos por essas disciplinas.

Estratégias como a recuperação de incidentes, o treinamento de conscientização, a recuperação de desastres e o planejamento de continuidade de negócios tornaram-se componentes básicos da estrutura operacional das organizações. Diante da ocorrência de um evento indesejado ou imprevisto que paralise ou comprometa os negócios de uma organização, essas estratégias permitirão recuperar o mais rapidamente os serviços afetados (SULE, 2014).

Porém, eventos indesejados e imprevistos podem gerar outros problemas, além da recuperação dos serviços, como, por exemplo, reclamações de seguro, ensejo a indenizações, ocorrência de crimes, entre outras questões legais e regulatórias. Pode haver processos judiciais contra colaboradores, terceiros prestadores de serviços ou contra a própria organização, referentes ao que ocasionou o incidente, bem como suas consequências. Nesse contexto, surge a importância do vestígio digital para as organizações que usam a infraestrutura de TI em seus negócios (SULE, 2014).

Tradicionalmente, a coleta e a análise dos dados que subsidiarão um processo forense são realizados após a ocorrência de um incidente. No entanto, Rowlingson (2004) argumenta que, no cenário da AFD e na maioria das discussões forenses, as organizações tendem a ignorar o que acontece com seus sistemas antes da decisão de empreender uma investigação. O vestígio poderá existir e ser encontrado, ou não existir e impossibilitar a investigação eficaz do incidente. Em geral, uma AFD é reativa, inicia quando um crime foi cometido ou descoberto e os investigadores comparecem à cena do crime.

Tais preocupações levaram à produção de recomendações para adoção, pelas organizações, de uma postura mais proativa em relação à análise forense digital, preparando seus sistemas, procedimentos e funcionários antes que um incidente ocorra, viabilizando a identificação, preservação e armazenamento dos vestígios digitais para as investigações. Essa abordagem tem sido referenciada por estudiosos do assunto e profissionais forenses como "digital forensic readiness" (DFR) (TAN, 2001). Os pesquisadores têm desenvolvido diversas propostas para sua implementação, alinhando políticas, sistemas e treinamentos de funcionários aos objetivos forenses.

Pretende-se demonstrar, neste trabalho, a importância da implementação da produção de informação forense proativa nas organizações, quer sejam governamentais ou privadas. Partindo-se de uma extensa análise da literatura, pretende-se, ainda, apresentar a evolução desse conceito, tanto no meio acadêmico como empresarial.

Este trabalho divide-se em cinco seções. A seção atual introduziu os conceitos e estabeleceu as diferenças entre análise forense digital e recuperação de incidentes, sobretudo para ressaltar a necessidade de as organizações adotarem uma postura forense digital mais proativa.

> *1 Neste trabalho, a despeito de todas as referências de pesquisas terem sido disponibilizadas em idioma inglês, optou-se por utilizar o termo "Vestígio Digital" em vez de "Evidência Digital", pelo fato de ser o termo reconhecido pela legislação e meio jurídico brasileiro para se referir ao objeto a ser periciado.*

A segunda seção apresenta o surgimento do conceito de "digital forensic readiness" e faz considerações sobre as possibilidades para a tradução da expressão para a língua portuguesa.

A terceira seção apresenta diversas abordagens sobre o tema, responsáveis por sua evolução e adoção xnos meios acadêmicos e organizacionais.

A quarta seção apresenta os benefícios decorrentes da adoção da *"digital forensic readiness"* pelas organizações em geral e a necessidade de amparo legal para sua instituição como ferramenta de suporte aos processos legais que envolvam investigações digitais.

A quinta seção conclui e propõe outros trabalhos práticos a serem realizados.

2- Histórico

Há o reconhecimento, entre os pesquisadores e a comunidade forense digital, que o termo e o conceito original de "digital forensic readiness" (DFR) foram cunhados por Tan (2001), em um relatório em que foram apresentadas medidas a serem incorporadas aos procedimentos de segurança existentes, com o objetivo de projetar redes e implementar sistemas com a finalidade de incrementar a "forensic readiness" (FR) de uma organização.

Nesse relatório, Tan (2001) definiu como elementos de DFR: a capacidade de um ambiente para produzir provas credíveis, a preservação dos vestígios e o tempo necessário para realizar uma análise forense, após a ocorrência um incidente, propondo técnicas de monitoramento de sistemas para maximizar a utilidade dos dados dos vestígios de incidentes e minimizar o custo da análise forense durante uma resposta a incidentes.

Desde então, o termo "digital forensic readiness" e seu conceito básico - "maximizar a habilidade de uma organização para coleta e uso do vestígio digital (admissível em tribunal) e minimizar o custo da análise forense nas respostas aos incidentes" – têm sido amplamente aceitos e adotados pela comunidade forense digital.

Embora seja desejável a tradução de termos técnicos para o português, o termo original em inglês foi mantido neste trabalho, por duas razões: a primeira, pelo fato de não ter sido encontrado nenhum artigo em língua portuguesa tratando sobre o assunto; a segunda, por mais óbvia que possa parecer a tradução do termo "forensic readiness" para "prontidão forense", é duvidosa a adequação dessa tradução para uma compreensão abrangente e imediata de seu significado.

Seguramente, novos trabalhos surgirão abordando o tema e a consagração da melhor tradução se dará pelo uso.

3 - Abordagens de DFR

Diversos estudos têm sido conduzidos abordando a DFR sob diferentes perspectivas.

Sob a perspectiva governamental e acadêmica, Mouhtaropoulos, Grobler e Li (2011) estenderam o conceito básico de DFR, considerando a necessidade de preparação dos sistemas, procedimentos, processos e colaboradores antes da ocorrência de um incidente, o que envolve a identificação, preservação e armazenamento do vestígio digital.

O Governo do Reino Unido - Her Majesty's Government (HMG) - destaca-se pela produção de padrões técnicos, leis, normas, políticas e guias, muitos dos quais servem de base para a formulação de padrões e normas internacionais. No âmbito governamental, a produção de uma política de FR é um requisito mandatório definido no HMG, Security Policy Framework (SPF: reference [c]).

Em 2015, foram publicados pelo CESG, o Good Practice Guide nº 18, Forensic Readiness (GPG 18), o qual cobre a formulação da política de FR e provê recomendações para sua implementação, e o IA Implementation Guide Forensic Readiness Planning, endereçado aos profissionais envolvidos na implementação de políticas e atividades de planejamento de FR.

Um recente estudo foi apresentado por Park *et. al.* (2018), no DFRWS 2018 Europe - Proceedings of the Fifth Annual DFRWS Europe, no qual se analisa o estado atual da legislação de proteção aos dados nos países: Austrália, Reino Unido, Canadá, Estados Unidos, Alemanha e Coreia do Sul. O trabalho se baseia no estudo de (MOUHTAROPOULOS *et al.,* 2011) tendo sido especificamente projetado para discutir a eficácia da atual legislação de proteção de dados, o impacto que a forense digital tem na segurança da informação e se

há benefícios na implementação da DFR de forma obrigatória, tomando-se como caso de estudo a implementação da DFR no Reino Unido.

Esse estudo, comparando as legislações de proteção aos dados dos países selecionados, mostra a necessidade de se desenvolver requisitos de segurança robustos, nas organizações públicas e privadas. A tabela abaixo, apresenta, em resumo, como o conceito de FR está se desenvolvendo no setor público de alguns países.

[2] *Digital Forensic Research Workshop.*

PAÍS	REINO UNIDO	ESTADOS UNIDOS	ALEMANHA	COREIA DO SUL
Obrigatório	Sim	Não	Não	Não
Diretriz / Melhores Práticas	Good Practice Guide Forensic Readiness (Outubro 2015)	NIST: Guide to Integrating Forensic Techniques into Incident Response (Agosto 2006)	Precaution for IT- Forensics (Maio 2017)	Guideline for Incident Response Readiness in Financial Businesses (Dezembro 2016)
Estrutura e Contexto do Guia	-Conceitos de forense digital -Conceitos de Forensic Readiness -Riscos sem Forensic Readiness -Benefícios com Forensic Readiness -Custos -Princípios comuns (comentado nos princípios, propósito, sugestão para adoção)	-Estabelecendo Capacidade Forense -Realizando o Processo Forense (Coleta de dados, Exame, Análise, Relatórios) -Usando os dados (livro-texto guia estilizado; explanação detalhada, exemplos) -Apêndices (Recomendações, Cenários)	- Objetivos -Referências para outros Guias (para Detecção, Gestão de Incidentes, etc.) -Requisitos Básicos -Requisitos padrões -Requisitos Avançados (não estado da arte)	-Conceito de Incident Response (IR) Readiness (focado na violação da Forensic Readiness) -Conceito de Forense Digital -Necessidade da IR Readiness -Modelo de IR Readiness (explanando em detalhes sobre ferramentas forenses, artefatos forenses, etc.)
Checklist	SIM (Avaliação de Capacidade, Conteúdo da Política de Forensic Readiness)	SIM (Organizando uma Capacidade Forense, Realizando a Análise Forense, Cenários)	Não	SIM (Checklist para IR em negócios financeiros)

Tabela 1 - Comparação de guias reconhecidos pelo governo para FR Fonte: Adaptado de Park et. al. (2018)

Sob a perspectiva de aumento da eficiência das investigações digitais, minimizando esforço na coleta e preservação de informações forenses robustas para posterior uso pela organização nos tribunais, Endicott-Popovsky, Frincke e Taylor (2007) propuseram uma metodologia para incorporar capacidades forenses a redes de comunicação, operacionalizando assim o DFR.

Neste trabalho, propõe-se evolução para as práticas forenses, para que, de naturalmente reativas, passem a incorporar algum nível de proatividade. Aponta-se também para a necessidade de se planejar a DFR no contexto das políticas de segurança da informação das organizações.

Isso pressupõe explicitar, incluir entre as políticas de gerenciamento de segurança digital "a disposição da organização de triunfar no tribunal", o que implicará necessidade de ampliação das funções dos administradores de redes de

comunicação e de sistemas, bem como no entendimento de como os requisitos legais para admissibilidade dos vestígios podem ser traduzidos em requisitos para os sistemas de informação – por exemplo, onde e quais dados da rede coletar, como e quais ferramentas e procedimentos utilizar; quem deve ser treinado e em quais tópicos etc. Enfatizando-se que a simples adoção de uma ferramenta ou técnica não será suficiente.

Os pesquisadores em ciências forenses ao redor do mundo têm apoiado os esforços de DFR propondo que as organizações implementem políticas e processos (ROWLINGSON, 2004), gerenciem e monitorem os recursos humanos e técnicos alinhados aos objetivos forenses, Reddy e Venter (2013), e promovam o correto treinamento dos funcionários (ROWLINGSON, 2004).

Sob a perspectiva de frameworks para DFR, vários estudos têm sido publicados, como, por exemplo, o framework definido por Valjarevic e Venter (2011) que propõe um modelo e um conjunto de orientações e procedimentos para serem seguidos quando da implementação de DFR para sistemas de infraestrutura de chaves públicas (PKI). Destaca-se, pela abrangente análise da literatura, desde que o termo "digital forensic readiness" foi introduzido pela primeira vez por Tan (2001), o estudo conceitual realizado por Elyas et al. (2015), no qual foram identificados e catalogados 70 artigos publicados entre os anos de 2001 e 2012.

Os autores buscaram compreender e descrever a forensic readiness organizacional, identificando três capacidades distintas, objetivos de DFR que uma organização deve ter: demonstração de conformidade regulatória; investigações internas; e vestígios que podem ser utilizados em processos legais (gestão de vestígios legais).

No framework teórico de DFR proposto por Elvas et al. (2015), as capacidades forenses são sustentadas por dez fatores principais, elementos identificados que influenciam e contribuem para a DFR organizacional.

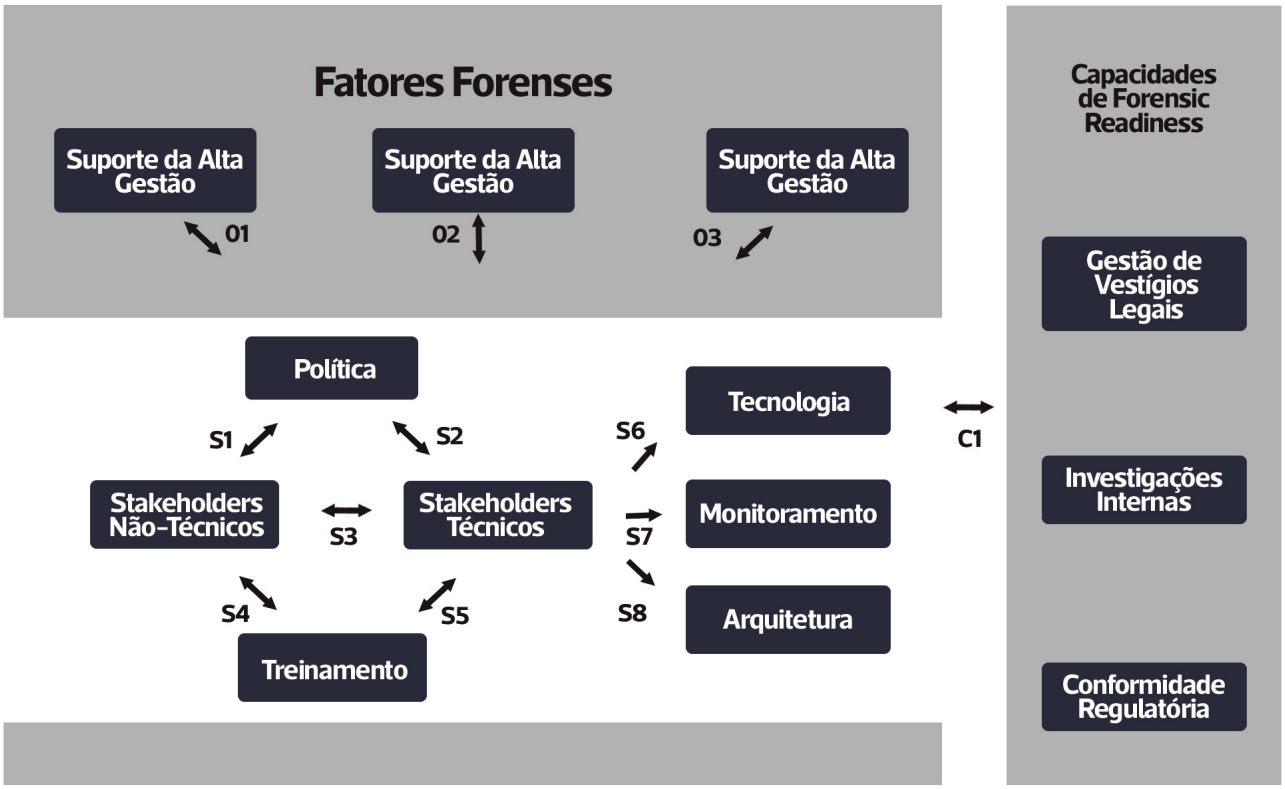

Figura 1 - Framework Proposto para Digital Forensic Readiness Organizacional
Fonte: Adaptado de "Framework of Organizational Digital Forensic Readiness", Elvas et al (2015)

Sete fatores são críticos ao elaborar uma estratégia forense: stakeholders não técnicos, stakeholders técnicos, tecnologia, monitoramento, arquitetura, política e treinamento.

Três fatores são organizacionais, externos ao programa forense, influenciam o desenvolvimento e a implementação da estratégia forense: cultura forense, apoio da alta administração e governança.

Sob a perspectiva das questões e desafios em torno da implementação da DFR nas organizações, Karie e Karume (2017) apresentam diferentes medidas proativas que as organizações podem adotar como forma de aumentar a capacidade de responder a incidentes de segurança e criar um ambiente digital pronto para a análise forense.

Nesse artigo, são examinados os problemas e desafios relativos à retenção e disposição de dados nas organizações, o que também pode ter alguns efeitos sobre a implementação da DFR. Isso é apoiado pelo fato de que, embora a necessidade de provas forenses digitais nas organizações tenha sido explorada, como a necessidade de DFR dentro das organizações, os tomadores de decisão ainda precisam entender o que é, de fato, necessário realizar em suas organizações para garantir sua implementação.

Sob a perspectiva de como os sistemas de software implantados nas organizações podem ser projetados para serem eles próprios forensic readiness (FR), Pasquale et al. (2018) investigaram requisitos de FR sobre sistemas de software e suposições sobre a abrangência desse ambiente, a fim de derivar especificações de software implementáveis com vistas à FR.

O estudo é focado na relação entre engenharia de software e FR, partindo da constatação que o centro da FR são os dados digitais: mídias e informações de logs de atividades disponíveis nos sistemas de informação da rede de uma organização ou nos dispositivos dos usuários, que podem conter informações valiosas, especialmente associadas à linha de tempo, eventualmente permitindo determinar como ocorreu um incidente e seu perpetrador, que viabilizarão à organização ser bem-sucedida em um processo administrativo ou judicial contra o agressor.

Um conjunto de requisitos centrados em dados e no processo foi eliciado, visando garantir a disponibilidade, a relevância, a minimalidade, as ligações entre os dados, a completude, o não repúdio, a procedência e a conformidade legal das informações mantidas.

Foram identificados, também, desafios da engenharia de open software, enfatizando que é necessário se construir um consenso em torno das principais características de um sistema de software FR e, no futuro, haverá necessidade de se caracterizar formalmente sistemas FR. São feitas considerações sobre a necessidade de se adaptar os métodos de engenharia de software existentes para atenderem aos requisitos de FR, o que gera uma nova questão: Como verificar se os sistemas de software existentes atendem aos requisitos de FR?

Como última e não trivial questão, endereçada pelos autores às pesquisas da engenharia de software, são propostos os desafios decorrentes dos próprios desenvolvimentos tecnológicos, citando-se, como exemplo, a crescente disseminação de dispositivos da internet das coisas (IoT) e do software embarcado nesses dispositivos.

Ainda na linha de pesquisa da FR na engenharia de software, pesquisadores têm discutido uma estratégia alternativa denominada forensic-by-design, caracterizada pela integração de requisitos forenses nas principais fases do ciclo de vida de desenvolvimento de sistemas.

Um estudo realizado por Grispos et al. (2017) propôs examinar até que ponto as organizações realmente implementam essa abordagem, forensic-by-design, para obter a FR, realizando uma pesquisa on-line para analisar a perspectiva da indústria.

Sob a perspectiva de serviços em FR, algumas organizações especializadas em segurança da informação e respostas a incidentes já agregam a implementação da FR em seus portfólios de serviços, oferecendo não apenas a implementação lógica e física, mas também expertise em combate a fraudes e outros crimes digitais para nichos específicos de mercado (CRAVEN et al.,2016), (PwC Thailand Forensic Services, 2018), (QUEST, 2018).

Os resultados da pesquisa, juntamente com os resultados da literatura analisada, levaram os autores a reconhecer uma série de desafios de pesquisa para a eliciação explícita de requisitos forenses, análise e implementação de tais requisitos nos sistemas a serem construídos.

Dada a existência de variados estudos sobre DFR, observa-se que o tema ganha gradativa relevância, tanto no contexto acadêmico como no das organizações.

4 - Benefícios da adoção da DFR

Embora a definição original de FR: "maximizar a habilidade de uma organização para coleta e uso do vestígio digital (admissível em tribunal) e minimizar o custo da análise forense nas respostas aos incidentes" (TAN, 2001), seja, ainda, amplamente utilizada e referenciada nas publicações sobre o assunto, com a publicação do Good Practice Guide Forensic Readiness No. 18, CESG (2015), instituiu-se a seguinte redefinição, que tem sido também utilizada em diversas publicações: "obtenção, por uma organização, de um nível adequado de capacidade para que seja apta a coletar, preservar, proteger e analisar os vestígios digitais, para que esses vestígios possam ser efetivamente usados em qualquer assunto legal, em questões disciplinares, tribunais de trabalho ou de justiça."

Comparando-se as duas definições, observa-se que o CESG (2015) desenvolve uma visão mais ampla do que seria essa "habilidade de uma organização", apontando uma possível gradação dessa "habilidade" quando define "um nível adequado de capacidade", o que leva a crer que organizações diferentes, possuem necessidades diferentes de FR e que, sua implementação deve se dar na medida justa de suas necessidades negociais, ou seja, podem coexistir na esfera governamental do Reino Unido diferentes níveis de FR, contanto que as organizações observem as orientações estabelecidas pelos guias, normativo e operacional, que disciplinam a matéria.

De acordo com o CESG (2015), as organizações devem selecionar um nível de capacidade de FR e requisitos de política de acordo com diversos fatores aplicáveis aos seus ambientes de Tecnologia da Informação e Comunicação (TIC).

A tabela abaixo apresenta as recomendações CESG (2015) para políticas e capacidades de FR, uma abordagem escalonada com os níveis de 1 a 5 (colunas) representando uma escala crescente.

INCREMENTO DA CAPACIDADE

Fator	Nível 1	Nível 2	Nível 3	Nível 4	Nível 5
Segmentação do modelo alvo	CONSCIENTE	DETER		DETER E RESISTIR	DEFENDER
Orientações para políticas de Forensic Readiness	• Consciência do benefício da FR. •Capacidade construída de maneira reativa em resposta a eventos. • As fontes de capacidades extrínsecas são identificadas proativamente. • Ser um assinante WARP ativo. • Conformidade com as regula-mentações sobre as práticas comerciais licitas (manter informadas as equipes de monitora-mento). • Capacidade de responder às demandas FOIA , DPA e de divulgação.	Nível 1 mais: • Propriedade da FR formalmente estabelecida. •Plano documentado e sujeito a simulações anuais pelo órgão. •Contrato formal de nível de serviço com provedores de serviços extrínsecos. •Primeiros interventores treinados. •Existência de plano de continuidade do negócio. •Capaz de instituir demandas RIPA .	Nível 2 mais: • Capacidade intrínseca limitada para apoiar investigações internas. • Auditorias regulares • Gestão dos registros eletrônicos auto-auditável. • Treinamento para a equipe de resposta e para aqueles que podem precisar apresentar registros nos tribunais. • Equipe de resposta a incidentes e inscrição no GovCERTUK .	Nível 3 mais: • Caso formal e tratamento de evidências. • Profissionais competentes (investigado-res e especialis-tas). • Gestão dos registros eletrônicos auditados anualmente segundo BS 10008:2008. **Polícia:** • Aplicações e ordens em conformidade com PACE e SOCPA . • Busca e aprensão. **Justiça Criminal** • Processos criminais	Nível 4 mais: • Colabora-ção transfron-teiriça (anti cyber crime) • Operações secretas e suporte de inteligência.
Capacidades internas típicas	•Nenhuma.	•Primeiros a responder.	• Equipe interna de resposta a incidentes com capacidade forense digital limitada.	• Capacidade forense digital abrangente. Apenas para a Polícia: • Capacidade adicional para todos os tipos de perícia e cenas de investigações criminais.	•Ampla capacidade de suportar grandes investiga-ções e coleta de informações.

Capacidades internas típicas	•Nenhuma.	•Primeiros a responder.	• Equipe interna de resposta a incidentes com capacidade forense digital limitada.	• Capacidade forense digital abrangente. Apenas para a Polícia: • Capacidade adicional para todos os tipos de perícia e cenas de investigações criminais.	•Ampla capacidade de suportar grandes investiga-ções e coleta de informações.
Capacidade de infraestrutura técnica típica	•Nenhuma.	•Nenhuma.	• Ferramentas de forense digital. • Captura de Log. • Intensificar o monitoramento para suporte a investigações.	• Arquivos das comunicações eletrônicas empresariais. • Agentes forenses digitais au-tomatiza-dos nos servidores.	• Laborató- rios de pesquisas. • Intercepta-ção.
Capacidades externas típicas	• Fornecedo-res identifica-dos • Encaminha-mento de questões criminais suspeitas à aplicação da lei (universal a todos os níveis).	• Fornecedo-res retidos e linha de ajuda.	• Fornecedores contratados com especialistas de plantão.	• Capacidade de substituição dos fornecedores intrínseca. • Testemunhas peritas indep-en-dentes.	• Confiança na aplicação da lei estrangeira para casos trans-fron-teiriços.

[1]WARP (Warning, Advice and Reporting Point) - serviço baseado em uma comunidade em que onde os membros podem receber e compartilhar conselhos atualizados sobre ameaças, incidentes e soluções de segurança da informação.

[2] Lei de Liberdade de Informação, de 2000, fornece acesso público às informações mantidas pelas autoridades pzúblicas.

[3] Lei de Proteção aos Dados, de 2018, controla como as informações pessoais são usadas por organizações, empresas ou pelo governo.

[4] Lei de Regulação dos Poderes Investigativos (RIP ou RIPA), de 2000, regulamenta os poderes dos órgãos públicos para realizar vigilância e investigação, e cobrir a interceptação de comunicações.

[5] Parte do Grupo de Comunicações e Segurança Eletrônica (CESG), equipe de resposta a emergências informáticas do governo do Reino Unido. Ajuda as organizações do setor público a responderem a incidentes de segurança informáticos e fornece recomendações para reduzir a exposição a ameaças.

[6] Lei dos crimes organizados graves e da polícia, de 2005, (frequentemente abreviado para SOCPA).

Tabela 2 - Níveis de capacidade de FR e requisitos de política
Fonte: Adaptado de CESG (2015) Apêndice A - Fatores de Capacidade

A definição original dada por Tan (2001) vincula à FR a capacidade de reduzir os custos de uma organização, associados às análises digitais forenses, o que não se pode, ainda, comprovar na prática, sobretudo pela necessidade de novos investimentos que uma implementação de FR pode demandar.

Na definição do CESG (2015), o fator financeiro não foi incluído para justificar a importância de se estabelecer esse processo nas organizações, reforça-se, no entanto, a importância de se preparar uma organização para disputas judiciais que são cada vez mais recorrentes, dada a crescente dependência das organizações em tecnologias digitais e, também, à própria democratização e desmitificação dessas tecnologias. Tal popularização torna os usuários corporativos menos inibidos e mais imprudentes no sentido de explorarem falhas e brechas de segurança em sistemas corporativos, o que pode propiciar ilícitos, os quais deverão ser tratados posteriormente pela organização.

O guia do CESG (2015) tem por objetivo ajudar as organizações governamentais, mas não se limita a elas, a atender aos requisitos de formulação de políticas de FR incluídos na Estrutura de Política de Segurança do HMG (SPF: reference [c]), HGM (2018), orientando o cumprimento normativo e instituindo a proatividade forense no âmbito governamental.

Vale destacar a introdução do guia CESG (2015) que afirma: "não se pode considerar como FR o investimento indevido em software forense digital de alto valor, contratos de fornecimento de serviços caros ou diversão para as pessoas espionarem aleatoriamente informações dos usuários em discos rígidos (que, se feitos incorretamente, seriam ilegais). A necessidade de implantar a perícia digital, para muitas or-

ganizações, será pouco frequente, mas é uma contingência que deve ser planejada."

A FR é uma resposta à necessidade, cada vez mais premente, das empresas se prepararem para litígios judiciais envolvendo tecnologia, análises forenses digitais e vestígios digitais.

O cenário econômico atual aponta para uma grande demanda de combate às fraudes em todas as sociedades. É crescente o número de empresas, organizações e países que estão reconhecendo que a corrupção e a fraude estão impedindo-as de competir no cenário global – essas práticas simplesmente ficaram muito dispendiosas para serem ignoradas.

A Pricewaterhouse Coopers (PwC), reconhecida prestadora de serviços em auditoria e consultoria, realiza anualmente a pesquisa "Global Economic Crime and Fraud Survey", e o relatório de 2018, denominado "Pulling fraud out of the shadows" apresenta dados significativos de mais de 7.200 respondentes em 123 países diferentes (PWC, 2018).

Porém, esses números foram considerados controversos pelos analistas que realizaram a pesquisa. Por exemplo, apenas 49% das organizações declararam terem sido vítimas de fraude ou crime econômico, entretanto, a percepção dos analistas é de que esse número deveria ser muito maior. O que dizer dos 51% que não se declararam vítimas? A realidade é que poucas empresas estão plenamente conscientes dos riscos relacionados a fraudes a que estão expostas.

Hoje, a luta contra as fraudes tornou-se uma questão central para os governos e para os negócios, não sendo mais vista como um incidente isolado de mau comportamento, um incômodo caro ou um mero problema de conformidade. Isso porque a escala e o impacto das fraudes cresceram significativamente, ônus de um mundo digitalmente dependente.

De fato, a fraude quase pode ser vista como um grande negócio - tecnologicamente habilitado, inovador, oportunista e abrangente, podendo ser pensado como a maior concorrente que uma empresa desconhecia ter.

Nesta era de incomparável escrutínio público, as organizações enfrentam numerosos riscos relacionados a fraudes: internos, externos, regulatórios e de reputação. Portanto, sugere-se que seja o momento oportuno para a adoção de uma visão moderna e mais holística sobre as fraudes, que reconhece a verdadeira forma da ameaça e não apenas um custo próprio de fazer negócios, mas uma indústria de sombra que pode afetar todos os territórios, todos os setores e cada função.

Ocorrida a fraude, pensa-se em seguida em identificação e responsabilização dos envolvidos, por meios legais, daí a ênfase na aceitabilidade legal dos vestígios. As organizações estão começando a obter valor de tecnologias alternativas e disruptivas no combate às fraudes. O gráfico abaixo, mostra a utilização de alguns desses métodos nas capturas de vestígios.

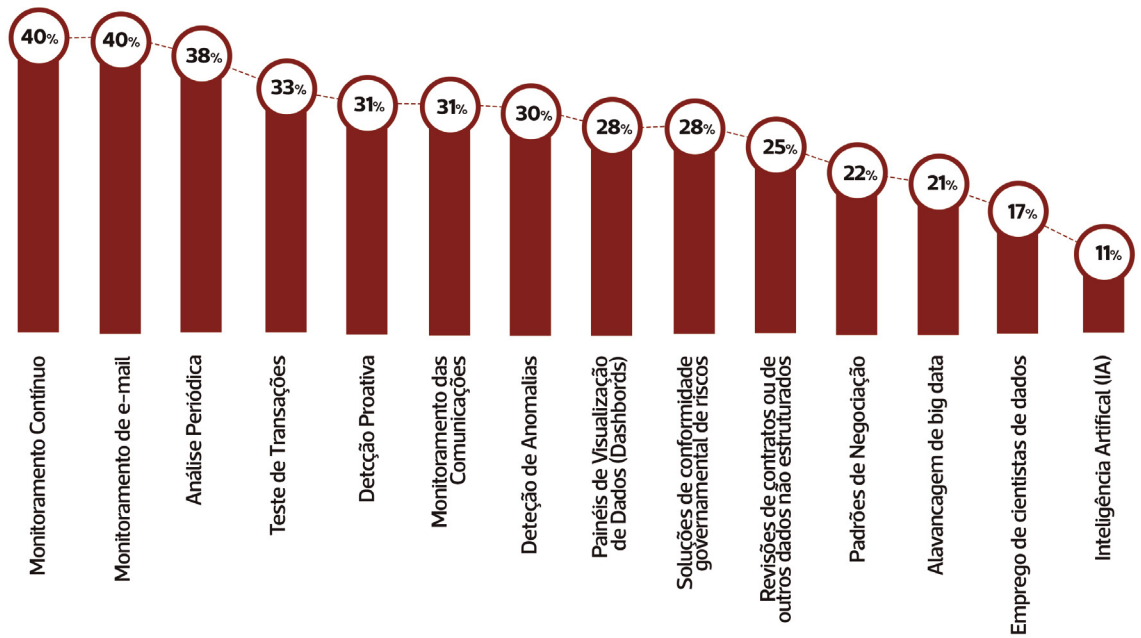

Figura 2 –Uso de Tecnologias alternativas e disruptivas no combate à fraude
Fonte: Adaptado de Global Economic Crime and Fraud Survey (PWC, 2018).

A FR é uma maneira das organizações se prepararem para embates judiciais, e assim, a implementação de qualquer tecnologia alternativa e disruptiva precisa ser planejada de modo a garantir a cadeia de custódia, chamada de "continuidade da evidência" no Reino Unido.

A cadeia de custódia garantirá que os vestígios digitais sejam coletados, processados, manuseados, armazenados e protegidos, de tal forma que não sejam alterados ou destruídos, ou que não sejam inferidos. Envolve, também, a documentação de quem lidou com os vestígios e por quê - do ponto de coleta até a apresentação como uma exibição, por exemplo, nos tribunais ou em processos disciplinares internos às organizações.

A forense digital pode também ser usada em processos de auditorias e pode ser muito útil para investigar fraudes. Os auditores podem usar ferramentas e técnicas forenses para monitorar e revisar a conformidade com políticas organizacionais e requisitos regulatórios.

Ter um plano de FR em vigor é um bom caminho para garantir tais investigações, e qualquer descoberta pode ser tratada e apresentada para que a organização tenha sucesso, caso seja necessário ir aos tribunais.

5 - Conclusão

A crescente frequência, sofisticação e letalidade dos ataques cibernéticos estão estimulando as empresas a procurar maneiras mais estruturadas para evitá-los. A abordagem "forensic readiness" tem o benefício adicional de permitir um foco mais profundo na prevenção de fraudes.

Embora alguns países, como os EUA, Reino Unido e Canadá, entre outros, estejam na vanguarda em relação a "forensic readiness", não se pode afirmar que seja um conceito difundido e consolidado na comunidade forense digital global.

Diversos aspectos da "forensic readiness" são, ainda, suscetíveis a melhores definições decorrentes dos avanços das pesquisas. Pode-se citar, por exemplo, a FR aplicada à engenharia de software, orientada aos requisitos negociais passíveis de ataques e fraudes de uma organização.

Esse aspecto é especialmente interessante no contexto de combate à corrupção e malversação de recursos públicos. Por exemplo, diversas práticas habituais de agentes públicos são conduzidas corriqueiramente de forma a privilegiar pessoas ou grupos de seus interesses, sem contudo gerarem rastros passíveis de análises que possibilitem aperfeiçoar os controles e a transparência dessas ações, em muitos casos sem haver registro material da trocas desses "favores" por pagamento de propinas, possibilitadas simplesmente pela fragilidade dos sistemas informáticos que não incorporam requisitos forenses quando de seus desenvolvimentos.

Assim como é possível identificar por meio de algoritmos, para os mais variados fins, o comportamento das pessoas que se conectam à internet, analisando os registros de navegação, e a partir dessas análises produzir conteúdo de interesses específicos, publicidade e negócios, as organizações podem igualmente se beneficiar com a adoção de mecanismos que lhes permitam identificar comportamentos e ações maliciosas em suas redes corporativas e no uso de seus sistemas, para combatê-los proativamente.

No decorrer das pesquisas realizadas, observou-se que o setor privado e as organizações públicas caminham para a resposta proativa às ameaças cibernéticas, e a DFR é um componente importante para atingir essa meta.

No futuro, a política e os planos de FR, além do histórico de implementação, poderão demonstrar a posição de uma organização sobre sua governança corporativa, sobretudo em relação às fraudes que envolvem crimes do colarinho branco, de lavagem de dinheiro e de corrupção. Essa posição, também, poderá ser vista positivamente pelos tribunais.

A fim de fomentar a adoção da forensic readiness nas organizações que prestam serviços ao governo, as legislações que disciplinam os acordos de leniência poderiam ser revistas no sentido de tornar a implementação da forensic readiness um possível item desses acordos, visando garantir a intenção das organizações de combaterem internamente as fraudes, subornos, lavagem de dinheiro e outros crimes econômicos. Dessa forma, esses acordos poderiam ser mais

flexíveis com as organizações que se predisponham a adotar a FR dentro de prazos determinados.

No âmbito governamental, diversos mecanismos de coleta e de armazenamento de vestígios forenses em sistemas desenvolvidos para suportar atividades fins poderão ser instituídos por meio de regulamentação, o que expandirá a capacidade de auditoria e controle do Estado. A exemplo da experiência do Reino Unido, a DFR possivelmente deva ser instituída como requisito obrigatório para o setor governamental.

Embora o conceito apresentado neste trabalho não tenha ainda uma normatização internacional própria, as normas ISO série 27000, normatizam alguns aspectos concernentes à FR, como, por exemplo, a ISO/IEC 27037 que diz respeito à captura inicial de vestígios digitais; a ISO/IEC 27041 que oferece orientação sobre os aspectos de garantia da perícia digital, por exemplo, assegurando que os métodos e ferramentas apropriados sejam usados adequadamente; a ISO/IEC 27042 abrange o que acontece após a coleta de vestígios digitais, ou seja, sua análise e interpretação; e a ISO/IEC 27050 que diz respeito a eletronic discovery.

O conceito de forensic readiness apresenta-se como abordagem capaz de colaborar significativamente para elevar os índices de resolução de crimes cibernéticos, para estabelecer um nível de governança de dados e informações mais efetivo, para instituir transparência de gestão e para fortalecer as organizações nos embates judiciais relacionados aos crimes digitais ocorridos no âmbito de seus domínios.

A base do conceito é identificar, manter e garantir que evidências digitais, sistematicamente coletadas pelas organizações em processos cotidianos, preventiva e proativamente, sejam reconhecidas e validadas nos tribunais.

Por fim, pode-se inferir a FR como uma tendência no campo da análise forense digital que, embora tenha um longo caminho de estruturação e maturação a percorrer, conceitualmente já se apresenta razoavelmente justificável, dadas especialmente as questões relacionadas à governança, ao desejo de mitigação de corrupção e de fraudes nos negócios globais e à proteção das organizações no complexo contexto das demandas judiciais.

Referências

CESG. Good Practice Guide 18 Forensic Readiness. 2015. Disponível em: https://www.ncsc.gov.uk/content/files/guidance_files/GPG%2018%20-%20Forensic%20Readiness%20-%20Issue%201.2%20-%20Oct%2015%20-%20NCSC%20Web.pdf

CESG. IA Implementation Guide Forensic Readiness Planning. 2018.

CRAVEN, Clem, WILSON, Ian e SCOTT, Matthew. Practical Forensic Readiness in Security Operations. 2016. Disponível em: https://www.first.org/resources/papers/conf2016/FIRST-2016-44.pdf

ELYAS, Mohamed, AHMAD, Atif, MAYNARD, Sean e LONIE, Andrew. Digital Forensic Readiness: Expert Perspectives on a Theoretical Framework. Computers & Security. 52. 10.1016/j.cose.2015.04.003. 2015. Disponível em: https://www.researchgate.net/publication/275157238_Digital_Forensic_Readiness_Expert_Perspectives_on_a_Theoretical_Framework

ENDICOTT-POPOVSKY, Barbara, FRINCKE, Deborah A. e TAYLOR, Carol A. A Theoretical Framework for Organizational Network Forensic Readiness. Journal of Computers. 2. 10.4304/jcp.2.3.1-11. 2007. Disponível em: https://www.researchgate.net/publication/42803345_A_Theoretical_Framework_for_Organizational_Network_Forensic_Readiness

FREILING, Felix C. e SCHWITTAY, Bastian. A common process model for incident response and digital forensics. 2007. Disponível em: https://www.imf-conference.org/imf2007/2%20Freiling%20common_model.pdf

GRISPOS, George, GARCÍA-GALÁN, Jesus, PASQUALE, Liliana, NUSEIBEH, Bashar. Are you ready? Towards the engineering of forensic-ready systems. 2017. In 11th IEEE International Conference on Research Challenges in Information Science, 2017, In Press. Disponível em: https://arxiv.org/pdf/1705.03250.pdf

HMG. Security Policy Framework, Version 1.1. 2018. Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/710816/HMG-Security-Policy-Framework-v1.1.doc.pdf

HOOGSTRATE, Andre. Are you ready? Forensically speaking - On digital forensic readiness. 2014. Disponível em: http: / / leidensafetyandsecurityblog.nl/ articles/ are-you-ready-forensically-speaking-ondigital-forensic-readiness

[10] KARIE, Nickson menza 275404 e KARUME, Simon Maina Dr. Digital Forensic Readiness in Organizations: Issues and Challenges. Journal of Digital Forensics, Security and Law: Vol. 12: No. 4, Article 5. 2017 Disponível em: https://commons.erau.edu/cgi/viewcontent.cgi?article=1436&context=jdfsl

MOUHTAROPOULOS, Antonis, GROBLER, Marthie e LI, Chang-Tsun. Digital Forensic Readiness: An Insight into Governmental and Academic Initiatives. Proceedings. European Intelligence and Security Informatics Conference, EISIC 2011. 191 - 196. 10.1109/EISIC.2011.30. Disponível em: https://www.researchgate.net/publication/224264483_Digital_Forensic_Readiness_An_Insight_into_Governmental_and_Academic_Initiatives

NHS DIGITAL. Forensic Readiness Good Practice Guide. 2017. Disponível em: https://digital.nhs.uk/services/data-and-cyber-security-protecting-information-and-data-in-health-and-care/cyber-and-data-security-policy-and-good-practice-in-health-and-care/forensic-readiness-guidance-for-health-and-care-organisations/forensic-readiness-good-practice-guide

PARK, Sungmi, AKATYEV, Nikolay, JANG, Yunsik, HWANG, Jisoo, KIM, Donghyun, YU, Woonseon, SHIN, Hyunwoo, HAN, Changhee e KIM, Jonghyun. A comparative study on data protection legislations and government standards to implement Digital Forensic Readiness as mandatory requirement. 2018. Disponível em: https://www.sciencedirect.com/science/article/pii/S1742287618300446

PASQUALE, Liliana, ALRAJEH, Dalal, PEERSMAN, Cláudia, TUN, Thein Than, NUSEIBEH, Bashar, e RASHID, Awais. Towards Forensic-Ready Software Systems. 2018. In ICSE-NIER'18: 40th International Conference on Software Engineering: New Ideas and Emerging Results Track, May 27-June 3, 2018, Gothenburg, Sweden. ACM, New York, NY, USA, 4 pages. 2018. Disponível em: https://www.researchgate.net/publication/322696770_Towards_Forensic-ready_Software_Systems

PWC 2018a. Global Economic Crime and Fraud Survey. 2018. Disponível em: https://www.pwc.com/gx/en/forensics/global-economic-crime-and-fraud-survey-2018.pdf

PWC 2018b. Thailand Forensic Services. Forensics Services Brochure.

2018. Disponível em: https://www.pwc.com/th/en/consulting/forensic/assets/brochure-forensic-services-brochure-2018.pdf [17] QUEST. Mapping your requirements to the NIST Cybersecurity-framework white-paper-26571. 2018. Disponível em: https://www.quest.com/whitepaper/mapping-your-requirements-to-the-nist-cybersecurity-framework8134595/

REDDY, K. e VENTER, H. S. The architecture of a digital forensic readiness management system. 2013. Computers & Security Volume 32, February 2013, Pages 73-89. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167404812001447

ROWLINGSON, Robert. A ten step process for forensic readiness. 2004. International Journal of Digital Evidence, vol. 2, no. 3, pp. 1–28. Disponível em: https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B13342-B4E-0-1F6A-156F501C49CF5F51.pdf

[20] SULE, Dauda. Importance of Forensic Readiness. 2014. Disponível em: https://www.isaca.org/Journal/archives/2014/Volume-1/Pages/JOnline-Importance-of-Forensic--Readiness.aspx

TAN, John. Forensic Readiness. Artigo, 2001. Disponível em: https://isis.poly.edu/kulesh/forensics/forensic_readiness.pdf

US-CERT. Computer Forensics. 2008. Disponível em: http://www.us-cert.gov/reading_room/forensics.pdf

VALJAREVIC, Aleksandar e VENTER, H. S. Towards a digital forensics readiness framework for public key infrastructure systems. Information Security South Africa, pages 1-10, Johannesburg, South Africa: IEEE. 2011. Disponível em: https://www.researchgate.net/publication/224259134_Towards_a_Digital_Forensic_Readiness_Framework_for_Public_Key_Infrastructure_systems