UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

O USO DO PROCESSO DE E-DISCOVERY COMO FORMA DE APRIMORAMENTO DA SEGURANÇA DA INFORMAÇÃO

MICHEL GOMES NOGUEIRA

ORIENTADOR: HÉLVIO PEREIRA PEIXOTO

DISSERTAÇÃO DE MESTRADO EM ENGENHARIA ELÉTRICA
ÁREA DE CONCENTRAÇÃO INFORMÁTICA FORENSE E SEGURANÇA DA INFORMAÇÃO

PUBLICAÇÃO: PPGENE.DM - 624/2016

BRASÍLIA / DF: DEZEMBRO/2016

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

O USO DO PROCESSO DE E – DISCOVERY COMO FORMA DE APRIMORAMENTO DA SEGURANÇA DA INFORMAÇÃO

MICHEL GOMES NOGUEIRA

DISSERTAÇÃO DE MESTRADO SUBMETIDA AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE BRASÍLIA, COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE.

APROVADA POR:

HÉLVIO PEREIRA PEIXOTO, Dr., DPF
(ORIENTADOR)

FLÁVIO ELIAS GOMES DE DEUS, Dr., ENE/UNB
(EXAMINADOR INTERNO)

LAERTE PEOTTA DE MELO, Dr., BANCO DO BRASIL
(EXAMINADOR EXTERNO)

Brasília, 07 de dezembro de 2016.

FICHA CATALOGRÁFICA

NOGUEIRA, MICHEL GOMES
O uso do processo de e-Discovery como forma de aprimoramento da Segurança da Informação [Distrito Federal] 2016.
(xiii), (123)p., 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2016).

Dissertação de Mestrado – Universidade de Brasília, Faculdade de Tecnologia. Departamento de Engenharia Elétrica.

1. e-Discovery 2. Segurança da Informação
3. Evidência digital

I. ENE/FT/UnB. II. Título (Série)

REFERÊNCIA BIBLIOGRÁFICA

NOGUEIRA, Michel G. (2016). O uso do processo de e-Discovery como forma de aprimoramento da Segurança da Informação. Dissertação de Mestrado, Publicação PPGENE.DM - 624/2016, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, (123)p.

CESSÃO DE DIREITOS

NOME DO AUTOR: Michel Gomes Nogueira
TÍTULO DA DISSERTAÇÃO: O uso do processo de e-Discovery como forma de aprimoramento da Segurança da Informação.
GRAU/ANO: Mestre/2016.

Michel Gomes Nogueira
Universidade de Brasília
Campus Universitário Darcy Ribeiro – Asa Norte
CEP 70.910-900 – Brasília – DF - Brasil

Ao grande Espírito Santo, Conselheiro, Amigo. A majestade pertence a Ti e só a Ti. O que recebemos é apenas uma partícula ínfima da sua incomparável e imensurável sabedoria.

À minha querida esposa Nara Fabiana, companheira em todos os momentos, sem a sua compreensão, suporte e apoio seria inviável a conclusão deste trabalho. Minha linda muito obrigado por toda a sua força! Amo você de paixão!

Ao meu querido filho Pedro, sempre especial, sempre importante e sempre amado. Pedro, você é um grande presente de Deus na minha vida. Amo você mais do que o infinito... e além!

Aos meus queridos pais, Altair e Virginia. Vocês me ensinaram a amar a Deus, a vida, ao próximo e a respeitar os livros. Amo vocês profundamente!

Aos meus irmãos, Marcelo, Bruno e Giordano. Ao longo do tempo vocês têm me ensinado como é importante aceitar as diferenças. Amo vocês!

Aos meus sogros, Satiro e Dalmina. Vocês têm agido como verdadeiros pais na minha vida. E a recíproca é verdadeira, me sinto como filho na família. Sempre os amarei!

AGRADECIMENTOS

Ao único e sempre eterno Deus.

A meu orientador Dr. Hélvio Pereira Peixoto, a minha profunda gratidão, pelo apoio, incentivo, dedicação, amizade para o desenvolvimento deste trabalho. Seus conhecimentos, sua inteligência e sabedoria foram fundamentais para ampliar a minha visão científica.

Aos Peritos Criminais Federais Marcelo de Azambuja Fortes e Delluiz Simões de Brito. Obrigado por todo o apoio e incentivo!

Aos colegas da Coordenação Geral de Tecnologia da Informação do Ministério da Justiça e da Polícia Federal, por todo apoio, amizade e incentivo para o desenvolvimento deste trabalho.

Aos colegas e professores do curso de Mestrado por tudo que passamos juntos.

Agradeço, especialmente, à minha amada e querida esposa Nara Fabiana e o meu filho Pedro. Todo o tempo dedicado a este projeto foi pensando em nossa família.

A todos, os meus sinceros agradecimentos.

O presente trabalho foi realizado com o apoio da Polícia Federal – PF com recursos do Programa Nacional de Segurança Pública com Cidadania – PRONASCI, do Ministério da Justiça.

RESUMO

O USO DO PROCESSO DE E-DISCOVERY COMO FORMA DE APRIMORAMENTO DA SEGURANÇA DA INFORMAÇÃO

Autor: Michel Gomes Nogueira

Orientador: Hélvio Pereira Peixoto

Programa de Pós-graduação em Engenharia Elétrica

Brasília, dezembro de 2016

O trabalho descrito nesta dissertação trata do uso do processo de e-Discovery para verificar as descobertas eletrônicas encontradas que podem evidenciar uma provável falha de segurança da informação, possivelmente gerando prejuízos financeiros, econômicos e à imagem da organização. A proposta deste trabalho é uma adaptação do processo de e-Discovery para a identificação, preservação, processamento, análise e produção de informações armazenadas eletronicamente, e que sirvam de proposta para aprimoramento de Sistema de Gestão de Segurança da Informação, bem como na sustentabilidade da Governança da Tecnologia da Informação – TI. A análise dos controles de Segurança da Informação, por meio da perspectiva do e-Discovery, pode contribuir com a identificação prévia de vulnerabilidades e com a capacidade da organização em coletar e preservar evidências relacionadas a um eventual processo de litígio de forma eficiente e com menores custos.

ABSTRACT

E-DISCOVERY AS A MEAN TO IMPROVE INFORMATION SECURITY

Author: Michel Gomes Nogueira

Supervisor: Hélvio Pereira Peixoto

Programa de Pós-graduação em Engenharia Elétrica

Brasília, December of 2016

The work described in this thesis deals with the use of the electronic discovery process for early identification of information security failure that can possibly generate financial/economic losses and / or damage to the organization's image. The proposed model involves the identification, preservation, processing, analysis and production of electronically stored information as a tool for improvement of the organization´s Information and Communications Security System, as well as the sustainability of Governance of Information Technology – IT. The analysis of the security controls through the perspective of the e-discovery can help early identification of vulnerabilities, improving the organization's ability to preserve and collect potentially relevant evidence in an efficient, cost-effective and defensible manner.

SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

LISTA DE SÍMBOLOS, NOMENCLATURA E ABREVIAÇÕES

ABNT – Associação Brasileira de Normas Técnicas

APF – Administração Pública Federal

CDN – Conselho de Defesa Nacional

CGTI – Coordenação Geral de Tecnologia da Informação

COBIT – Control objectives for Information and related Technology

DLOG – Diretoria de Logística

DSIC/PR – Departamento de Segurança da Informação e Comunicações da Presidência da República

EaD – Ensino a distância

EDRM – Eletronic Discovery Reference Model

EGD – Estratégica de Governança Digital

ESI – Eletronically Stored Information

FIRAC – Facts, Issues, Rules and References, Analysis and Conclusions

FRCP – Federal Rules of Civil Procedure

FRCrP – Federal Rules of Criminal Procedure

FRE – Federal Rules of Evidence

GED – Gestão Eletrônica de Documentos

GSI – Gabinete de Segurança Institucional da Presidência da República

IGRM – Information Governance Reference Model

LAI –Lei de Acesso à Informação

OCR - Optical Character Recognition

PF – Polícia Federal

SaaS – Software as a Service

SCI – Sistema de Controle Interno

SGSI – Sistema de Gestão de Segurança da Informação

TCU – Tribunal de Contas da União

TIC – Tecnologia da Informação e Comunicação

VoIP – Voice over Internet Protocol

1. INTRODUÇÃO

A era do Big Data deu início a uma explosão de dados em indústrias, incluindo saúde, ciência, infraestrutura, marketing, finanças, governo, justiça, segurança cibernética, dentre outros. Um dos desafios que essas organizações enfrentam atualmente é aproveitar o volume, a velocidade e a variedade de dados, a fim de criar informação sobre a qual podem ser realizadas decisões importantes. (ERIN, 2015).

O termo *e-Discovery* surge exatamente no contexto de grande volume de dados em meio digital, dados ainda não estruturados, submetido a um processo de descoberta eletrônica, pela qual se realiza uma tarefa de "mineração de dados" para seleção de informações relevantes que serão utilizados em procedimentos legais e disputas judiciais. Para processos criminais, o *e-Discovery* tende a focar na forense digital, em processos civis, o *e-Discovery* tende a estabelecer procedimentos bem definidos para estreitar a busca por informações relevantes em meio digital. (PHILLIPS et al., 2013).

Ocorre que, esses achados podem ser resultados de falhas de segurança da informação das organizações, fruto de uma política de segurança da informação mal elaborada, cujo controle de acesso à rede de dados, a informações sigilosas, ao serviço de internet e de e-mail é realizado de forma precária, sem uma visão holística do Sistema da Gestão de Segurança da Informação.

Conforme abordado por Nogueira (2011), os órgãos e entidades da Administração Pública Federal Direta e Indireta exibem um arcabouço de normas corporativas, as quais devem ser implementadas para fins de consolidação da Gestão de Segurança da Informação e Comunicações, em complementação àquilo estabelecido no ordenamento jurídico.

Atualmente compete ao Departamento de Segurança da Informação e Comunicações da Presidência da República – DSIC/PR, definir normativos e requisitos metodológicos para implementação de ações de segurança da informação e comunicação pelos órgãos e entidades da administração pública federal, no âmbito da Secretaria-Executiva do Conselho de Defesa Nacional - CDN. (BRASIL, 2015).

Ao todo são 21 normas complementares vigentes que estabelecem diretrizes para diversas ações de segurança da informação e comunicação no âmbito da Administração Pública Federal – APF.

Em relação à iniciativa privada não há obrigação em se estabelecer políticas e normativos relacionados à segurança da informação, é discricionária a decisão da organização

em elaborar suas próprias políticas. Entretanto, no que concerne as normas da ABNT, há um padrão para prover diretrizes em termos de segurança da informação que pode ser adotado e implementado tanto pelo setor público como pelo privado. Por exemplo: a norma ABNT NBR ISO/IEC 27001:2013, que trata da adoção de um Sistema de Gestão de Segurança da Informação – SGSI e a norma ABNT NBR ISO/IEC 27002:2013, que apresenta um código de prática para controles de segurança da informação.

1.1. PROBLEMA TRATADO (CONTEXTUALIZAÇÃO)

De acordo com o Relatório de Gestão da Polícia Federal de 2014[1], a estrutura de governança interna da PF tem por finalidade auxiliar o órgão no alcance dos objetivos institucionais. Para isso, a Polícia Federal conta com um Assessor de Controle Interno, cujas atribuições estão resumidas em: auxiliar a Direção-Geral em assuntos relacionados à aderência do órgão aos atos legais e normativos; à comunicação interna de decisões; à comunicação externa com órgãos diversos, sobretudo Controladoria-Geral da União - CGU e Tribunal de Contas da União - TCU.

Em 2014 o Plano Estratégico - PE 2010/2022 do DPF foi atualizado, incluindo como Objetivo Institucional "Consolidar a Governança em Tecnologia da Informação" (item 9.8 do PE), para fins de ampliar o grau de conformidade dos processos de TI para com as práticas de governança, particularmente as elencadas nos livros de ITIL e COBIT (item 9.8.1 – PE).

Tendo como base a recomendação do TCU ao Ministério da Justiça - MJ, Acórdão nº 1019/2014 – Plenário, o TCU destaca nos itens 90 e 95 do Acórdão que mesmo que o MJ não tenha uma unidade de auditoria interna, recomenda-se que sejam realizadas avaliações periódicas na área de tecnologia da informação do órgão, em especial no que diz respeito à avaliação da governança de TI, dos sistemas de informação e de suas bases de dados, da segurança da informação e das aquisições de bens e serviços de TI.

> 95. Recomendar ao Ministério da Justiça que, com base nas orientações contidas no Cobit 5, MEA02.03 - *Perform control self-assessments* (Realizar auto-avaliação dos controles– tradução livre), realize, por meio de uma área interna ou externa à TI, avaliações periódicas na área de tecnologia da informação do órgão, a exemplo da avaliação dos controles de governança de TI, do funcionamento dos sistemas de informação e de suas bases de dados e, dos processos relacionados à segurança da informação e às aquisições de bens e serviços de TI.

[1] Trabalhou-se com o Relatório de Gestão da Polícia Federal de 2014, pois o relatório referente ao ano de 2015 não foi publicado até o momento da conclusão da dissertação.

O Relatório de Gestão da Polícia Federal de 2014 destaca que o DPF não conta com uma unidade de auditoria interna em virtude da impossibilidade legal de adoção da mesma no âmbito da administração direta.

Essa situação provavelmente se modificará em razão da publicação da Instrução Normativa Conjunta nº 01, de 10 de maio de 2016, da Controladoria Geral da União – CGU, que dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal.

Segundo essa Instrução Normativa, os órgãos e entidades do Poder Público Federal deverão implantar atividades de controle interno de gestão, que são atividades materiais e formais, como políticas, procedimentos, técnicas e ferramentas, implementadas pela gestão para diminuir os riscos e assegurar o alcance de objetivos organizacionais e de políticas públicas.

Essas atividades podem ser preventivas (reduzem a ocorrência de eventos de risco) ou identificáveis (possibilitam a identificação da ocorrência dos eventos de risco), implementadas de forma manual ou automatizada.

O texto da norma ainda destaca que poderão ser realizadas avaliações específicas baseadas em métodos e procedimentos predefinidos, cuja abrangência e frequência dependerão da avaliação de risco e da eficácia dos procedimentos de monitoramento contínuo. Abrangem, também, a avaliação realizada pelas unidades de auditoria interna dos órgãos e entidades e pelos órgãos do Sistema de Controle Interno (SCI) do Poder Executivo federal para aferição da eficácia dos controles internos da gestão quanto ao alcance dos resultados desejados.

Atualmente na Polícia Federal encontra-se vigente a Portaria nº 01/2009 – CTI/DPF, de 14 agosto de 2009, que implementa atividades de Gerência de Segurança da Informação e tem, como uma de suas atribuições, auditorias periódicas de vulnerabilidades nos ativos de TI do DPF. A Portaria nº 35/2010 – CTI/DPF, de 29 de julho de 2010, dispõe sobre os critérios e procedimentos para o registro de incidentes de segurança da informação no âmbito do DPF e dispõe no art. 4º - parágrafo único que o registro do incidente de segurança da informação ocorrerá de maneira reativa. A Portaria nº 018/2013 – CGTI/DPF, de 08 de março de 2013, que dispõe sobre a realização de Auditoria Interna no âmbito da Coordenação-Geral de Tecnologia da Informação – CGTI/DPF, considera a necessidade de propor ações preventivas, corretivas e sugestões de melhoria, em acordo com o resultado de auditoria.

Conforme o artigo 24 e 25 da Política de Governança de TI do DPF, de 12 de janeiro de 2012, as metodologias de governança, os processos de trabalho, dentre outros instrumentos de promoção da qualidade e eficiência dos serviços de TI devem ser objeto de auditoria interna instituída no âmbito da CGTI/DPF.

A Política de Segurança da Informação do DPF, publicada por meio da Portaria nº 779/2009, de 18 de janeiro de 2010, impõe que devem ser estabelecidos procedimentos formais para notificação de falhas e incidentes de segurança da informação e mau funcionamento de equipamentos ou aplicativos.

Em suma, o que se verifica em linhas gerais é uma crescente necessidade de aprimoramento do controle interno dos órgãos da APF, com a utilização de atividades de auditorias internas, desenhada para adicionar valor e melhorar as operações de uma organização, auxiliando-a na realização de seus objetivos, a partir da aplicação de uma abordagem sistemática e disciplinada para avaliar e melhorar a eficácia dos processos de segurança da informação, de controles internos, de integridade e de governança.

> Compete às auditorias internas oferecer avaliações e assessoramento às organizações públicas, destinadas ao aprimoramento dos controles internos, de forma que controles mais eficientes e eficazes mitiguem os principais riscos de que os órgãos e entidades não alcancem seus objetivos. (BRASIL, 2016)

A questão que surge é que não se encontra, nem nos normativos vigentes do DPF e nem nos Acórdãos do TCU, qual ou quais modelos específicos poderiam ser usados pelos órgãos públicos para uso em Auditorias Internas em ambientes de Tecnologia da Informação que tratem, especificamente e de forma proativa, as possíveis vulnerabilidades de segurança da informação que possam comprometer os negócios da organização.

Essa é uma situação que não só afetam os órgãos governamentais, segundo Brito (2010), em vários lugares do mundo, existem milhares de executivos de TI preocupados em como encontrar a melhor forma de superar os principais desafios de gerenciar a TI, tornando-a um instrumento eficaz para o crescimento do negócio. Brito destaca a seguir alguns desses desafios:

- Racionalizar os custos da TI e demonstrar que se faz bom uso do orçamento;
- Contribuir de forma relevante para o negócio (inovações);
- Melhorar a eficiência dos processos de negócio (automatizar a operação);
- Atender auditorias, leis e marcos regulatórios; e

- Reduzir os riscos mantendo a segurança e a privacidade das informações mais críticas.

1.2. PROBLEMA TRATADO

Esta pesquisa aborda o problema relativo à ausência de qual ou quais modelos específicos podem ser usados de forma proativa pelos órgãos públicos para uso em Auditorias Internas em ambientes de TIC, particularmente àquelas que possam contribuir com a eliminação de possíveis vulnerabilidades de segurança da informação que comprometam a capacidade da organização em mitigar eventuais perdas em decorrência de uma possível ação judicial em razão do tratamento inadequado de informações.

Por não ser economicamente viável adotar o melhor modelo de segurança e armazenamento indiscriminado de todos os dados por um tempo indeterminado, uma priorização faz-se necessária, apontando quais dados são mais críticos do ponto de vista jurídico.

O problema, portanto, está na escolha de um modelo que possa sustentar as atividades relativas às auditorias internas em ambiente de tecnologia da informação e comunicação, cujo objetivo é minimizar possíveis riscos relacionados à segurança da informação que possam comprometer a capacidade da organização em atenuar prejuízos decorrentes de eventuais ações judiciais.

1.3. HIPÓTESE DE PESQUISA

É possível fazer uso de um modelo que se refere a descobertas eletrônicas e que tem como foco a produção de evidências digitais para uso de provas judiciais, também servir como instrumento de investigação/auditoria interna de uma organização para fins de aprimoramento da segurança da informação?

1.4. JUSTIFICATIVA E RELEVÂNCIA

Auditar, investigar e prover alternativas que promovam o aprimoramento da segurança da informação é função da governança de TI de qualquer organização para o cumprimento de sua função institucional, atendimento das áreas interessadas (cidadãos, clientes internos e externos, fornecedores, etc.) e estar em conformidade com às normas e à legislação vigente.

1.5. OBJETIVOS E ESCOPO

1.5.1. Objetivo Geral

Integrar o uso de um modelo voltado para descoberta digital no âmbito jurídico e aplicá-la na priorização da implementação de controles relativos à segurança da informação.

1.5.2. Objetivo Específico

No plano específico, o presente trabalho busca avaliar o modelo do processo de *e-Discovery*, analisar os pontos fundamentais para a sua aplicação no ambiente de tecnologia da informação; examinar os principais normativos de segurança da informação vigentes no Brasil (Política de Segurança da Informação e Comunicações; Política de Controle de Acesso, Política de Backup, etc); examinar os Acórdãos e normativos do Controle Interno e Externo dos órgãos/entidades da APF; analisar o fluxo de tratamento de incidentes de segurança da informação e as boas práticas do mercado para a Gestão da Segurança da Informação; estudar e relacionar os controles de segurança da informação das normas ABNT ISO/IEC 27001:2013 e 27002:2013 com o modelo do processo de *e-Discovery*; propor uma sistemática que permita a priorização da análise dos controles de segurança do Sistema de Gestão de Segurança da Informação de uma organização.

1.6. RESULTADOS ESPERADOS

Esse trabalho tem como objetivo apresentar os seguintes resultados:

- Levantamento dos normativos nacionais vigentes referente à *e-Discovery* e Segurança da Informação;
- Sugerir um modelo para priorizar o aprimoramento dos controles de Segurança da Informação;
- Contribuir com a divulgação de conceitos de *e-Discovery* para que organizações nacionais possam avaliar seus modelos de auditoria interna de Segurança da Informação; e
- Contribuir para aumento da eficiência no tratamento de incidentes de segurança da informação, em particular com aqueles relacionados às disputas judiciais.

1.7. MÉTODO DE TRABALHO

Para alcançar os objetivos propostos foram realizados os seguintes passos:

- Revisão da literatura relacionada ao processo de *e-Discovery*;
- Revisão da literatura relacionada à legislação e normativos referentes à Segurança da Informação e Direito Digital;
- Revisão sobre o Modelo de Referência de Descoberta Eletrônica (*Eletronic Discovery Reference Model – EDRM* [2]);
- Revisão das Normas ISO/IEC 27001:2013 e 27002:2013;
- Apresentação da relação entre o EDRM e as normas ISO/IEC 27001:2013 e 27002:2013, como proposta para priorização dos controles de segurança da informação; e
- Conclusões referentes às principais contribuições do processo *e-Discovery* para o aprimoramento da Segurança da Informação.

1.8. ORGANIZAÇÃO DA DISSERTAÇÃO

Os capítulos seguintes desta dissertação foram assim organizados: o Capítulo 2 apresenta a revisão de conceitos, destaque para *e-Discovery*, Governança de TI, Segurança da Informação, Forense Digital e Direito Digital. No Capítulo 3 é apresentada o modelo EDRM do processo *e-Discovery* que será relacionada com os controles de segurança da informação das normas ABNT NBR ISO 27001:2013 e 27002:2013. O capítulo 4 apresenta a priorização dos controles de segurança da informação resultante desta pesquisa, seguido do capítulo 5 com as conclusões finais e proposta de trabalhos futuros.

[2] Neste trabalho foi adotado o modelo que atualmente é gerenciado pelo Centro de Estudos Judiciais da Escola de Direito da Universidade de Duke em Durham, NC, nos Estados Unidos.

2. REVISÃO DE CONCEITOS

Este capítulo inicia com a revisão dos conceitos fundamentais necessários para o desenvolvimento da pesquisa. Como o processo de *e-Discovery* relaciona com outras áreas do mundo digital, torna-se indispensável a conceituação de temas pertinentes ao assunto. Em virtude disso, é essencial a compreensão de determinadas abordagens relacionadas ao tema *e-Discovery*, apresentadas na Seção 2.1; o histórico do *e-Discovery*, discutida na Seção 2.2; a governança de tecnologia da informação, a segurança da informação, a forense computacional, direito digital, abordados nas Seções 2.3, 2.4, 2.5 e 2.6, respectivamente. Na Seção 2.7 são realizadas as considerações finais deste capítulo.

2.1. E-DISCOVERY

Em se tratando da era digital, os dados são os mais importantes insumos que alimentam a produção da informação e conhecimento, propulsores modernos da economia pós-industrial. De acordo com Ferreira (2014) a sociedade da informação tem o seu histórico na consagração do código binário que desde o século XX iniciou a conversão de quase tudo em sequências combinatórias de zero e um, a fim de viabilizar a comunicação digital. Diversas ciências vêm atuando com novas dinâmicas de circulação da informação e do conhecimento, a partir do momento que sofrem interferências de elementos históricos, políticos, econômicos, sociais, legais, culturais e tecnológicos. A sociedade da informação está em constante mutação e é vivenciada de formas e maneiras diferentes de país para país, cada qual usufruindo de uma experiência heterogênea, afetados por investimentos empresariais e governamentais, em infraestrutura, número de habitantes conectados ou não à internet, tecnologias, telefonia, tamanho de banda, custos, qualidade de serviços e outras variáveis possíveis.

A difusão acelerada das novas tecnologias de informação e comunicação é um fator que tem que causado profundas transformações na economia mundial (TAKAHASHI, 2000) e no *modus operandi* das relações sociais.

> Ainda no caso do Brasil, este tem história na Sociedade da Informação, e no campo da segurança da informação e comunicações tem governança estabelecida, legislação vigente, vem construindo seu arcabouço normativo no âmbito do governo federal, e apesar de recente, se comparado ao arcabouço de leis, normas, padrões dos países desenvolvidos, tem destaque de atuação e reconhecimento nacional e internacional de sua competência em temas diretamente correlacionados à segurança cibernética. (CANONGIA E MANDARINO, 2009).

A descoberta (*discovery*) de documentos é um passo natural nos processos de litígios entre partes envolvidas num processo judicial. Compreende um procedimento pré-processual em que as partes de um litígio podem obter evidências documentais uma da outra, geralmente respondendo a perguntas, a interrogatório ou a pedidos de produção de documentos. De modo geral ocorre a troca de informações dispostas em documentos, que em última instância serão utilizados no julgamento da disputa em questão. (KAH, 2014).

Entretanto, o número crescente de documentos eletrônicos, como por exemplo, e-mails, planilhas eletrônicas, textos, apresentações, tem migrado a burocracia dos memorandos e livros para o formato digital. Com a implantação da Gestão Eletrônica de Documentos – GED objetivam-se a uniformização e digitalização de documentos e processos e redução do uso de papel.

> O uso da assinatura digital no Brasil, segundo o CEO da Destaque Tecnologia, Mário Scheel, é bastante disseminado e isso ajuda muito. "Os tribunais de Justiça são um bom exemplo. Culturalmente, o papel ainda tem muito crédito, mas existem países europeus muito mais atrasados que o Brasil nesta questão. Temos dois fenômenos recentes que mudaram nossa relação com a informação e vão ajudar na diminuição drástica do consumo de papel: a guarda de documentos em nuvem e a mobilidade", afirma e acrescenta que muita coisa já evoluiu e o Brasil está em consonância com o que acontece na maior parte do mundo. (MACIEL, 2015).

Segundo Maciel (2015), o Poder Judiciário do Brasil tem servido de exemplo da política de informatização dos tribunais com a tramitação de processos em meio digital e a gravação e realização de audiências por videoconferência.

E a questão retratada vem impactando o mundo tecnológico, que está se voltando cada vez mais para o conceito de *Big Data*[3], que é a transformação da informação em conhecimento. É a busca em dar sentido e utilidade aos dados inicialmente não estruturados utilizando técnicas capazes de analisar grandes volumes de dados de maneira individual. (MACIEL, 2015).

O processo de descoberta eletrônica (*e-Discovery)* tem exatamente o enfoque de buscar, dentro desse ambiente de dados estruturados ou não de uma organização (empresarial, governamental, não-governamental ou outras), informações que sejam relevantes para acesso ao espaço jurídico. Casey (2009) argumenta que o *e-Discovery* trata da "troca de dados entre as

[3] Big Data não trata apenas da dimensão de volume, como parece à primeira vista, mas existe também uma variedade imensa de dados, não estruturados, dentro e fora das empresas (coletados das mídias sociais, por exemplo), que precisam ser validados (terem veracidade para serem usados) e tratados em velocidade adequada para terem valor para o negócio. TAURION (2013). Segundo DeVan (2016) a fórmula para o Big Data são 7 V´s, ou seja, Big Data = volume + velocidade + variedade + variabilidade + veracidade + visualização gerando valor.

partes em um processo civil ou criminal". Os advogados dos litigantes determinam que dados devem ser fornecidos baseados na relevância ou nas alegações apresentadas.

Segundo Phillips et al (2013) "*e-Discovery* é o processo onde se busca utilizar informações em meio digitais como provas ou evidências eletrônicas". O conceito de evidência eletrônica engloba qualquer *Eletronically Stored Inf*ormation – ESI, informações armazenadas eletrônica ou digitalmente. Essas informações podem estar apostas em documentos, sistemas operacionais, e-mails, fotografias digitais, figuras, páginas em sítios da Internet, etc. O ESI está também presente nas memórias dos celulares, em discos rígidos, em mídias flexíveis como DVD´s e CD´s, bem como em todos os tipos de notebooks, computadores, *tablets*, *smart TV*, laptops e demais eletrônicos. De acordo com Phillips et al (2013) "*e-Discovery* pode ser pensada também como uma forma de mineração de dados para adquirir informações para uso em procedimentos legais".

Já a empresa de consultoria PWC (ca. 2016), refere-se ao *e-Discovery* como sendo "o processo de identificação, preservação, processamento, análise e produção de informações armazenadas eletronicamente". O propósito do *e-Discovery* é, portanto, o uso de documentos eletronicamente armazenados em processos judiciais. Segundo Hyman (2012), tradicionalmente, o uso de "*Discovery*" referia a documentação utilizada em um litígio judicial, mas que não era eletrônica, consistindo em um manual com o resumo dos documentos que eram requeridos e arrecadados entre as partes. A abrangência dos documentos eletronicamente armazenados é extensa e não se limita somente aos dispositivos supracitados, mas a todos os sistemas de computadores, dispositivos digitais e qualquer tipo de memória flash utilizada por empresas, indústrias, agências governamentais, escolas, hospitais, particulares, e que armazenam documentos eletrônicos (editor de texto, planilhas eletrônicas, agendas, calendários e apresentações), bem como as informações dispostas no *twitter*, *facebook*, *instagram*, *whatsapps*, etc.

O cumprimento de uma solicitação ou ordem judicial de *e-Discovery* é uma atividade importante, complexa, demorada e potencialmente cara. Sua abrangência na esfera judicial também pode envolver investigação criminal, consulta regulamentar ou apenas estar associada ao contexto de apresentação de informações para fins de conformidade regulatória. (PWC, ca. 2016).

2.2. HISTÓRICO DO E-DISCOVERY

O conceito de descoberta digital (*e-Discovery)* é considerado um conceito novo, embora possa se dizer que já se encontrava em prática, de forma não sistematizada, desde a década de 50. Com o surgimento dos *mainframes*, as informações eletrônicas começaram a ser progressivamente utilizadas em situações de litígio, principalmente em empresas que armazenavam dados financeiros, bancários, contábeis, comerciais, dentre outros. Nas décadas de 70 e 80, quando havia um litígio entre duas organizações, não havia disponibilidade de fornecer as informações armazenadas em mídias digitais. Geralmente as evidências apresentadas na corte de justiça pelos litigantes eram resmas de papel impressos, cuja quantidade de informação era menos que a produzida atualmente, mas a pilha de papel era alta o suficiente para intimidar qualquer oponente. (PHILLIPS et al., 2013).

Atualmente, o uso de termos como metadados[4], carimbo de tempo[5] (*timestamps*), análise de logs[6], funções de *hash*[7], se tornaram quesitos obrigatórios para qualquer exame forense.

Na década de 60, em plena guerra fria, nascia a ARPANET[8], a precursora da internet, tinha como objetivo inicial a criação de uma rede que fosse indestrutível aos bombardeios e que

[4] Muitos documentos e coleções de textos possuem metadados associados. Metadados contêm informação sobre a organização dos dados, seus domínios e relacionamentos. Metadados são "dados sobre os dados". Por exemplo, em um sistema de gerenciamento de dados, o esquema especifica alguns metadados, a saber, o nome das relações, os campos ou atributos de cada relação e o domínio de cada atributo. Metadados comumente associados a textos incluem o autor, a data de publicação, a fonte da publicação o tamanho do documento (em páginas, palavras, bytes) e o gênero do documento (livro, artigo, memorando). (BAEZA-YATES e RIBEIRO-NETO, 2013).

[5] O carimbo de tempo (ou *timestamp*) é um documento eletrônico emitido por uma parte confiável, que serve como evidência de que uma informação digital existia numa determinada data e hora no passado. O carimbo de tempo destina-se a associar a um determinado *hash* de um documento assinado eletronicamente ou não, uma determinada hora e data de existência. Ressalta-se que o carimbo de tempo oferece a informação de data e hora de registro deste documento quando este chegou à entidade emissora, e não a data de criação deste documento. A regulamentação do carimbo de tempo ICP-Brasil já foi aprovada pelo Comitê Gestor da ICP-Brasil. Há um conjunto de DOCs vigentes que regulamentam o tema, a saber: DOC-ICP-11, 12, 13 e 14. (ITI, 2012).

[6] Logs são informações sobre a situação de determinado elemento em um momento específico. Essas informações possuem informações históricas sobre a vida desses elementos. (COSTA, 2006).

[7] Funções Hash são geradas a partir de uma entrada de qualquer tamanho, uma saída de tamanho fixo, ou seja, é a transformação de uma grande quantidade de informações (informação original) em uma pequena sequência de bits (valor hash), de tal forma que não é possível retornar à informação original a partir de um valor hash. O que torna esse tipo de função extremamente utilizada para verificação de integridade de dados computacionais é o fato de que uma simples alteração na informação de entrada do algoritmo gerará uma sequência de bits (valor hash) completamente diferente. Assim, se o conteúdo de um arquivo é submetido a uma função unidirecional e, em seguida, seu conteúdo é alterado em um único bit e submetido novamente à mesma função, duas sequências de bits completamente diferentes serão obtidas como resultado da função de autenticação. (ELEUTÉRIO E MACHADO, 2011).

[8] ARPANET foi desenvolvida pela Advanced Research Projects Agency – ARPA. A futura rede deveria abranger todas as localidades das instituições financiadas pela ARPA, interligando seus computadores com sistemas de

interligasse pontos estratégicos para fins militares, ou seja, centros de pesquisa e tecnologia e serviços de informação nacional. A partir de 1990, o Departamento de Defesa dos Estados Unidos desmantelou a ARPANET e criou a NSFNET que se popularizou em todo o mundo, com a denominação da Internet, transformando-se num sistema mundial público de redes de computadores. A internet permitiu que qualquer pessoa ou computador, previamente autorizado, pudesse se conectar, e quando obtida a conexão, possibilitou a transferência de informação entre computadores. (BASÍLIO, 2006). O avanço tecnológico permitiu o surgimento de oportunidades de novos negócios e inovações de ferramentas de trabalho, mas também trouxe oportunidades para atuação de criminosos, principalmente com a disseminação do uso da internet.

Com o aumento da quantidade de ataques de hackers nos Estados Unidos, em 1984, o Congresso Americano aprovou uma lei criminalizando o acesso sem autorização aos computadores, conhecida como *Computer Fraud and Abuse Act* (CFAA)[9], (KERR, 2010). Mudanças adicionais no CFAA foram realizadas em 2001 e 2006 com a edição do "U.S. PATRIOT Act"[10]. (ESTADOS UNIDOS, 2001).

O uso do termo *e-Discovery*, como descoberta eletrônica, só se torna realmente popular no meio jurídico americano em 2001, com a repercussão de vários pedidos de falência de grandes empresas americanas, dentre elas se destacam a Enron[11], quando houve a necessidade de se investigar uma imensa quantidade de documentos digitais, incluindo os dados de e-mails dessas corporações, que o termo *e-Discovery* foi popularizado. Pois até esta data o entendimento que se tinha de e-*Discovery* era a simples conversão das informações em papel para um formato digital, com o objetivo de integrar os autos do processo judicial. Até então, a

tempo compartilhado, com o objetivo de reduzir os custos de transmissão, aumentar a confiabilidade e, potencialmente, ampliar os objetivos militares nas pesquisas em torno do assunto. (CARVALHO, 2006).

[9] A CFAA foi estabelecida em 1986 por meio da emenda 18 U.S.C § 1030 leia-se "U.S. Code Title 18 Section 1030" (KERR, 2009).

[10] Conhecida como Lei Patriótica é uma lei americana promulgada após os ataques terroristas de 11 de setembro de 2011, que permite o uso de grampo telefônico e monitoramento dos usuários da internet (DICTIONARY, 2016) para fins investigatórios. O ato determina e pune atos terroristas nos Estados Unidos e ao redor do mundo, e reforça o uso de ferramentas investigatórias para o cumprimento da lei. (ESTADOS UNIDOS, 2001).

[11] Empresa americana de energia com sede em Houston, Texas, que entrou com pedido de falência em dezembro de 2001. O colapso da Enron surpreendeu a maioria dos investidores e analistas, porque a Enron, a sétima maior corporação nos Estados Unidos, há muito tempo vinha relatando enormes ganhos financeiros. Investigações posteriores revelaram que a Enron tinha inflado seus ganhos e ocultado suas dívidas e perdas com suas subsidiárias parceiras. Embora alguns dos principais executivos da empresa tivessem adquiridos enormes lucros quando a Enron quebrou, muitos de seus funcionários viram as suas economias para aposentadoria dizimada pelo colapso do preço das ações da Enron. (DICTIONARY, 2016).

maioria dos casos de crimes que envolvia a necessidade de documentos eletrônicos era tratada pelo enfoque da forense digital. (PHILLIPS et al., 2013).

Essa série de escândalos financeiros resultou na aprovação da legislação Sarbanes-Oxley Act[12] (SOX como é conhecida no Brasil) e alteração na lei *Health Insurance Portability and Accountability Act* – (HIPPA)[13], esta última referente à portabilidade e responsabilidade de Seguros de Saúde

Em relação à SOX, trata-se de uma legislação que visa garantir mecanismos de auditoria e segurança confiáveis nas empresas, a fim de mitigar riscos aos negócios, evitar a ocorrência de fraudes, garantindo a transparência na gestão das empresas. Essa lei tem como um dos seus requisitos digitalizar e armazenar todos os documentos que estejam em papel, mantendo a guarda dos documentos de contabilidade, auditoria e de trabalho pelas empresas por até 7 anos. (SILVA, 2016).

De acordo com Ross (2015) "uma das principais seções da SOX, seção 404, entrou em vigor em 15 de novembro de 2004". Essa seção exige uma avaliação da estrutura de controles internos e dos relatórios financeiros para as empresas listadas em bolsa de valores nos Estados Unidos. Observa-se que a legislação americana se preocupa em informar aos acionistas, por meio de relatórios financeiros e auditorias, a situação de "saúde" da empresa. Fazendo uma relação com a Política de Governança Digital brasileira, o governo se propõe também a uma prestação de conta no uso dos serviços públicos, a fim de aprimorar os níveis de transparência e efetividade.

> (...) III – governança digital - a utilização pelo setor público de recursos de tecnologia da informação e comunicação com o objetivo de melhorar a disponibilização de informação e a prestação de serviços públicos, incentivar a participação da sociedade no processo de tomada de decisão e aprimorar os níveis de responsabilidade, transparência e efetividade do governo. (BRASIL, 2016)

Um caso judicial de grande repercussão nos Estados Unidos ocorreu em 2005, quando a fabricante de microprocessadores *Advanced Micro Devices* (AMD) acusou a Intel de práticas anticompetitivas. A justiça americana solicitou às litigantes uma imensa quantidade de documentos eletrônicos. Conforme citado por Losey (2009) as litigantes reconheciam que esta

[12] Em resposta aos escândalos corporativos como a Enron, WorldCom, Tyco e Adelphia em 2002, o Congresso do Estados Unidos promulgou a Lei Sarbanes-Oxley. A lei mais conhecida como "Sarbox" (no Brasil, como SOX), destina-se a proteger os investidores norte-americanos dos abusos corporativos. (ROSS, 2015).

[13] HIPPA é um lei federal americana de 1996, cuja última modificação ocorreu em agosto de 2002, que adotou padrões nacionais com o objetivo de proteger as informações dos prontuários dos pacientes e a especificar outros direitos privados (ESTADOS UNIDOS, 2016).

disputa poderia gerar a maior produção de documentos eletrônicos de toda história, correspondente a uma pilha de papel de 137 milhas, cerca de 220 quilômetros de altura.

Em resumo, a Figura 2.1 apresenta uma linha do tempo das leis que resultaram no processo *e-Discovery*. Ao todo foram quase 20 anos para que o termo se consolidasse no meio jurídico americano.

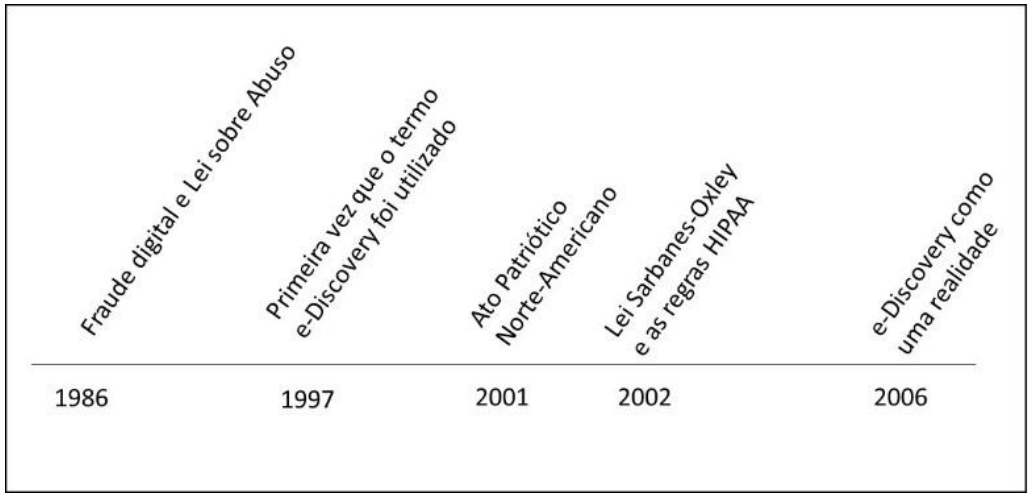

Figura 2.1- Linha do Tempo do e-Discovery (PHILLIPS et al., 2013, tradução)

2.3. GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO

A Norma ABNT NBR ISO/IEC 38500:2009 define a Governança Corporativa de TI como sendo "o sistema pelo qual o uso atual e futuro da Tecnologia da Informação e Comunicação - TIC é dirigido e controlado". De acordo com Cobit 5, considerado um modelo de negócios e de gestão global para governança e gestão de TI corporativa, a governança de TI lida com a crescente quantidade de informação digital e a forma como as organizações gerenciam essas informações para tomadas de decisões. (ISACA, 2016). Para o Cobit 5 "a governança garante que as necessidades, condições e opções das Partes Interessadas sejam avaliadas a fim de determinar objetivos corporativos acordados e equilibrados". O que possibilita que sejam realizadas as devidas tomadas de decisões e as priorizações dos objetivos estabelecidos.

Para a Norma ABNT NBR ISO/IEC 38500:2009, é importante que os dirigentes governem a TI através de três tarefas principais:

a) avaliar o uso atual e futuro da TI;

b) orientar a preparação e a implementação de planos e políticas para assegurar que o uso da TI atenda aos objetivos de negócio; e

c) monitorar o cumprimento das políticas e desempenho dos planos.

A Figura 2.2 ilustra o relacionamento dessas três tarefas principais com o meio externo, pressões do negócio e as necessidades do negócio; e com o meio interno, planos, políticas, propostas, desempenho, conformidade, processos do negócio, projetos de TI e operações de TI.

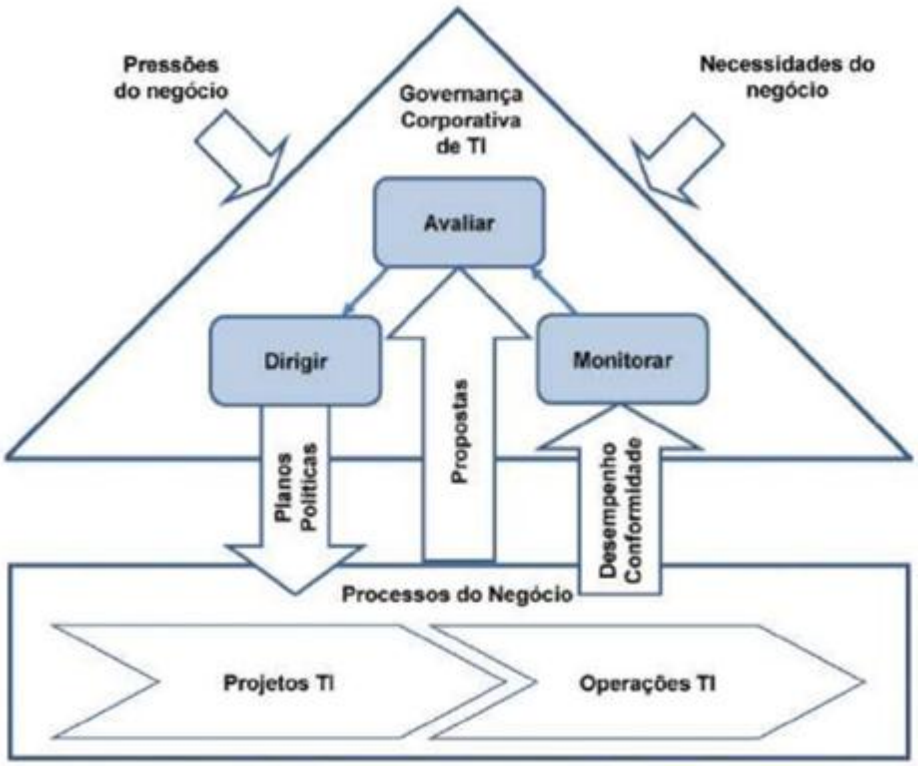

Figura 2.2- Modelo para Governança Corporativa de TI (ABNT, 2009)

O Governo Brasileiro vem trabalhando para aprimorar as suas políticas de TI, em particular no que tange à governança. Destaca-se que o Tribunal de Contas da União – TCU tem defendido que a governança de TI consiste no estabelecimento de mecanismos para assegurar que o uso da TI agregue valor ao negócio das organizações, com riscos aceitáveis, a fim de atender não somente a missão institucional da organização, mas também das diversas partes interessadas, que podem ser afetadas pelas decisões relacionadas à TI. (BRASIL, 2014).

Já o Sistema de Administração dos Recursos de Tecnologia da Informação – SISP (BRASIL, 2015), vinculado ao Ministério do Planejamento, Desenvolvimento e Gestão - MP, em seu Guia de Governança de Tecnologia da Informação e Comunicação, propõe que a

governança de TIC avalie e direcione o seu uso para dar suporte à organização e monitore seu uso para realizar os planos, incluindo a estratégia e as políticas de uso da TIC dentro da organização.

Recentemente, o Governo Federal publicou o Decreto nº 3.638/2016, do dia 15 de janeiro de 2016, que trata sobre a Estratégia de Governança Digital, cujo um dos objetivos é aprimorar os níveis de responsabilidade, transparência e efetividade do governo com a utilização pelo setor público de recursos de tecnologia da informação e comunicação, buscando a melhoria na disponibilização de informação e prestação de serviços públicos, incentivando a participação da sociedade no processo de decisão. (Brasil, 2016).

Para fins de exemplificação sobre a Governança de TI da PF, a Coordenação Geral de Tecnologia da Informação – CGTI/DLOG/PF instituiu em seu Planejamento Estratégico da TI, triênio 2015-2017, o tema governança de TIC com o objetivo de melhorar o desempenho operacional por meio da adoção das boas práticas de planejamento e organização das atividades de TIC. (Brasil, 2015).

A governança de TI tende a colaborar com o processo de *e-Discovery*, uma vez que planos, políticas e práticas de segurança da informação são geralmente implementadas à medida que a organização alcança maior maturidade em governança, atendendo assim aos eventuais requisitos presentes nas fases para descoberta eletrônica.

Deste modo, o processo *e-Discovery* se junta a governança com a proposta de contribuir para o aprimoramento das práticas de TI das instituições, uma vez que o uso dos dados eletrônicos de forma organizada e planejada possibilita uma resposta satisfatória aos questionamentos jurídicos, com um custo e tempo reduzido e em conformidade com a política de governança de TI. Quanto maior o nível de maturidade em governança de TI de uma organização subentende-se que melhores serão os resultados adquiridos por meio do processo de *e-Discovery*.

2.4. SEGURANÇA DA INFORMAÇÃO

A informação se tornou um fator diferencial para o mundo dos negócios, o seu poder de atuação é considerado um recurso fundamental para todas as organizações e a tecnologia desempenha um papel significativo desde o momento que a informação é criada até o momento em que ela é destruída. As organizações bem-sucedidas reconhecem que a TI é tão importante como qualquer outra área da organização. (ISACA/ COBIT5, 2012). Pensar no papel da

Segurança da Informação (disciplina da Governança de TI) é pensar na proteção de um dos ativos vitais de qualquer instituição.

A Segurança da Informação e Comunicações, conforme a Instrução Normativa GSI/PR nº 01, de 13 de junho de 2008, objetiva viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações. (Brasil, 2008). Segundo a norma ISO/IEC 27000:2016 (E), que trata da visão geral e do vocabulário dos termos e definições do Sistema de Gestão de Segurança da Informação, outras propriedades podem estar envolvidas com a segurança da informação, tais como responsabilidade, o não repúdio e a confiabilidade.

Atualmente órgãos e entidades da Administração Pública Federal Direta e Indireta possuem uma série de normas complementares, que devem ser implementadas para a realização da Gestão de Segurança da Informação e Comunicações, no que tange ao estabelecido no ordenamento jurídico.

Nesse sentido o Gabinete de Segurança Institucional da Presidência da República estabelece que as instituições governamentais devem remeter os resultados consolidados dos trabalhos de auditoria de Gestão de Segurança da Informação e Comunicações para o GSI, bem como atuar no tratamento de incidentes de segurança de informação. (Brasil, 2008).

Concomitante aos normativos do GSI, as normas ABNT NBR ISO/IEC 27001:2013 e 27002:2013 apresentam uma série de controles e objetivos de controles, necessários para implementar as opções de tratamento do risco da segurança da informação, os quais são:

- A.5 Políticas de segurança da informação;
- A.6 Organização da segurança da informação;
- A.7 Segurança em recursos humanos;
- A.8 Gestão de ativos;
- A.9 Controle de acesso;
- A.10 Criptografia;
- A.11 Segurança física e do ambiente;
- A.12 Segurança nas operações;
- A.13 Segurança nas comunicações;
- A.14 Aquisição, desenvolvimento e manutenção de sistemas;
- A.15 Relacionamento na cadeia de suprimento;
- A.16 Gestão de incidentes de segurança da informação;
- A.17 Aspectos da segurança da informação na gestão da continuidade do negócio; e

- A.18 Conformidade.

A proteção das informações está intimamente relacionada às práticas de governança e consequentemente podem se interligar a um processo de *e-Discovery* da organização, pois partindo do pressuposto que esta organização gerencia suas informações e tem o controle sobre os dados trafegados em sua rede de dados, qualquer ponto de vulnerabilidade detectado será um fator de risco no ambiente computacional. Sendo assim, os dados identificados como críticos no processo de *e-Discovery* poderão ser úteis para uma ação de proteção com vistas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações. E com isso, o processo de *e-Discovery* poderá alterar a dinâmica de atuação da governança de TI no sentido de se trabalhar de forma preventiva a identificação e o tratamento de falhas de segurança da informação passíveis de uma futura ação judicial por parte de um terceiro.

2.5. FORENSE COMPUTACIONAL

Tendo em vista que o *e-Discovery* tem como objetivo permitir e facilitar a análise de documentos e registros armazenados em meios eletrônicos com fins de compor um processo de litígio ou investigação corporativas complexas, há que se perguntar qual sua relação com a forense computacional.

A forense computacional é o processo que se utiliza de técnicas científicas para coletar, analisar e preservar uma evidência digital perante os tribunais de justiça. A disciplina computação forense combina elementos de direito e ciência da computação como forma de busca de informações digitais que possam ser usadas como prova em um processo judicial. (CERT-US, 2008).

O principal objetivo da Computação Forense, segundo Eleutério e Machado (2011), é:

> (...) determinar a dinâmica, a materialidade e auditoria de ilícitos ligados à área de informática, tendo como questão a identificação e o processamento de evidências digitais em provas materiais de crime, por meio de métodos técnico-científicos, conferindo-lhe validade probatória em juízo.

Para Casey (2011) a evidência digital pode ser qualquer dado eletrônico que indique que um crime foi cometido ou que pode ser um ponto de ligação entre o crime e as suas vítimas ou entre o crime e o executor. As evidências digitais podem ser extraídas de hardware e software de computadores, tais como sistemas digitais, disco rígido, memórias flash, documentos eletrônicos, unidades de armazenamento, etc.

Já para Pladna (2008) computação forense é a aplicação de investigação computacional, que analisa técnicas para determinar o potencial legal da evidência encontrada. Ou seja, a computação forense atua na captura de informações importantes que poderão ser utilizadas para apurar um crime digital.

Outro conceito é apresentado pelo Federal Bureau of Investigation – FBI, cuja computação forense é uma ciência que foi criada para atender uma necessidade específica da legislação, o que inclui técnicas de aquisição, preservação, recuperação e apresentação dos dados que estavam armazenados em mídia de computador para produção de provas eletrônicas. (NOBLETT, 2000).

Enfim, de acordo com Wiles et al. (2007) existem diversas definições para forense computacional, mas a sua favorita advém de Dan Farmer e Wietse Venema, que a define como coleta e análise de dados mais livre possível de distorções e preconceitos com a finalidade de reconstrui-los e mostrar o que aconteceu com esse dado dentro do sistema, "provendo um testemunho claro e objetivo e relatando os resultados da investigação".

É evidente que existe ao menos uma intersecção entre a forense computacional e o *e-Discovery*: a busca por dados e informações importantes que poderão ser utilizadas para elucidar um evento.

Como forma de enriquecimento das informações deste item, buscou-se além da conceituação, repassar alguns dos princípios norteadores da forense digital e o desencadeamento para o *e-Discovery*, conforme apresentados por Casey (2011) a seguir:

- *Evidence Exchange* (Troca de Evidência): Basicamente a Teoria de Locard ou o Princípio de Locard[14] - bastam que apenas dois pontos de evidência sejam necessários para relacionar o ofendido com a cena do crime. Nesse caso, a evidência digital pode revelar a comunicação entre o (s) suspeito (s) e a (s) vítima (s). As atividades *online* podem ser o fator chave para a descoberta de evidências.

> "(...) qualquer que sejam os passos, quaisquer objetos tocados por ele, o que quer que seja que ele deixe, mesmo que inconscientemente, servirá como uma testemunha silenciosa contra ele. Não apenas as suas pegadas ou dedadas, mas o seu cabelo, as fibras das suas calças, os vidros que ele porventura parta, a marca da ferramenta que ele deixe, a tinta que ele arranhe, o sangue ou sêmem que deixe. Tudo isso, e muito mais, carrega um testemunho contra ele. Esta

[14] O Princípio de Locard é aplicável na cena de crime, na qual o (s) interveniente (s) entram em contato com a própria cena onde o crime foi executado, trazendo algo relevante para a cena do crime. Cada contato deixa então o seu rastro. Os fragmentos das provas são qualquer tipo de material deixado pelo criminoso (ou tirada pelo mesmo) na cena do crime, ou o resultado do contato entre duas superfícies, tais como sapatos e o soalho ou solo. Miranda (2014).

> prova não se esquece. É distinta da excitação do momento. Não é ausente como as testemunhas humanas são. Constituem, per se, em uma evidência factual. A evidência física não pode estar errada, não pode cometer perjúrio por si própria, não se pode tornar ausente. Cabe aos humanos procurá-la, estudá-la e compreendê-la, apenas os humanos podem diminuir o seu valor". (LOCARD *apud* MIRANDA, 2014)[15].

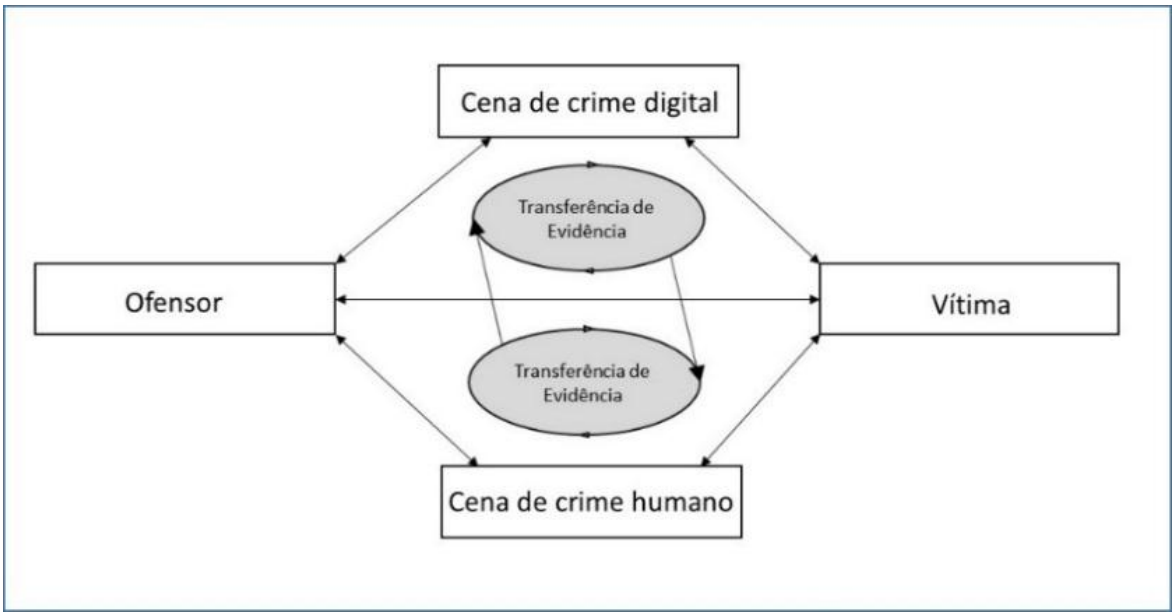

Figura 2.3 - Troca de Evidência seja na dimensão física ou digital (CASEY, 2011, tradução)

Segundo Auler et al. (2011) o princípio de Locard é um dos mais importantes ligados à informática forense, "qual a simples passagem do tempo pode provocar mudanças em um sistema de informática ativo".

> Isto ocorre devido a processos em execução, dados gravados ou apagados da memória, conexões de rede sendo criadas ou finalizadas, e assim por diante. O uso adequado de ferramentas de coleta de dados pelo Perito, embora agravem esta situação, não adicionam nenhuma evidência ao sistema.
> Todas essas pequenas alterações não produzem grandes consequências no sistema como um todo e podem ser explicadas posteriormente, através do exame minucioso e detalhado do material coletado. As modificações são produzidas pela interação das ferramentas com o sistema operacional do Windows, interferindo apenas com os arquivos do sistema operacional, não acarretando nenhuma mudança importante no conteúdo dos dados salvos no sistema. (AULER et al, 2011).

[15] LOCARD, EDMOND. Balística Forense – do Criminalista ao Legista. 1ª Ed. Rio de Janeiro: Editora Rubio, *apud* MIRANDA, 2014.

- *Evidence Characteristics* (Características da Evidência): as evidências geradas podem pertencer às seguintes categorias: evidências com atributos conhecidas como *class characteristics*, que são características com traços comuns para itens semelhantes, exemplo: tipo de vegetação, solo (pH), flora e fauna; e *individual characteristics*, que são características únicas, que podem estar relacionada a uma pessoa ou uma atividade específica com grande chance de certeza, exemplo: impressão digital, arcada dentária, DNA, etc.

- *Forensic Soundness* (Respeito aos preceitos forenses): esse princípio trata da possibilidade de alteração da evidência original em razão do processo pelo qual a evidência será submetida, o que não inviabiliza a veracidade do resultado encontrado. Casey exemplifica relatando o processo de análise do DNA, o material coletado original que pode ser uma mancha, um arranhão, etc, ao ser submetido aos testes laboratoriais sofre destruição, pois é inerente ao processo de análise de DNA. Essa situação também é inerente ao processo de forense digital, ao se coletar dados de um disco rígido, mesmo quando se utiliza um bloqueador de escrita, altera-se o estado original do disco. Tais alterações podem fazer com que áreas ocultas no disco se tornem acessíveis ou atualizadas pela "*Self-Monitoring, Analysis and Reporter Technology*" (SMART). A maioria dos métodos de coleta de informações de memórias de sistemas ativos (em funcionamento) ou dispositivos móveis sofrem alterações ou subscrição de parte da memória, o que é geralmente aceito na prática da forense digital. Em alguns casos, a corte americana vem obrigando a preservação dos dados da memória volátil. O autor cita o exemplo de um caso judicial entre duas empresas: Columbia Pictures Indum versus Bunnel. A corte solicitou que fossem mantidas as informações da memória RAM de um determinado servidor WEB que podia conter informações relevantes presentes nos dados de log.

  De acordo com Casey, a chave para que uma evidência não seja descartada perante a justiça é que se mantenha toda a documentação, a começar da origem da evidência e dos métodos de manuseio. Do ponto de vista da forense, o processo de coleta deve alterar o mínimo possível a evidência original e qualquer alteração, por menor que seja, deve ser documentada e avaliada dentro de um

contexto de resultado analítico final, de forma que a integridade e autenticidade possam ser validadas.

- *Authentication* (Autenticação): do ponto de vista legal, autenticação é o processo que determina se uma evidência é válida. Para a justiça interessa saber se o conteúdo coletado é de fato original, sem possibilidade de ter sido alterado ou manipulado; e se as informações de data e horário se mantêm corretas. Após o cumprimento dos pré-requisitos, determina-se a probabilidade de utilização da evidência.

- *Chain of Custody* **(**Cadeia de Custódia[16]): um dos pontos mais importantes do princípio da autenticação é a manutenção e a documentação da cadeia de custódia de uma evidência. Para o tribunal, a evidência apresentada deve ser a mesma evidência processada durante a investigação. A quebra da cadeia de custódia pode invalidar uma evidência que foi tratada de forma inconveniente.

- *Evidence Integrity* (Integridade da evidência): o objetivo da integridade é garantir que não houve alteração da evidência a partir do momento (data e hora) de sua coleta, de forma a manter o processo de autenticidade. Um exemplo disso é a função *hash* criptográfica, sendo que a troca de apenas um bit do material questionado é o suficiente para alteração da função de *hash*.

- *Objectivity* **(**Objetividade): o cerne da análise forense é a objetividade. Casey destaca que a interpretação e a apresentação da análise devem se abster de qualquer tipo de tendência para que os julgadores tenham uma visão mais clara possível dos fatos, sem noções pré-concebidas ou sem a pressão externa para alcance de uma interpretação específica. A maneira mais fácil de manter a objetividade é deixar a evidência "falar" por si mesma da melhor forma possível.

- *Repeatability* (Repetível): pode ser que ocorra a necessidade de que uma análise forense seja repetida e verificada por outro perito, de forma independente, para

[16] Em síntese, a cadeia de custódia representa um registro cronológico que objetiva documentar os acontecimentos relacionados as evidencias, desde sua coleta até sua apresentação em juízo. Visa a idoneidade da prova (COSTA, 2012).

> confirmação do resultado encontrado ou para que novas conclusões possam ser identificadas. No Brasil, o Código Processual Civil - CPC do Brasil, Lei nº 13.105/2015, o juiz nomeará perito especializado no objeto da perícia e fixará de imediato o prazo para a entrega do laudo (art. 465). Enquanto que as partes poderão indicar assistente técnico para acesso e o acompanhamento das diligências e dos exames que realizar, com prévia comunicação (§2º art. 466). Os assistentes técnicos são de confiança da parte e não estão sujeitos a impedimento ou suspeição (§ 1º art. 466). As partes também podem, de comum acordo, escolher o perito, indicando-o mediante requerimento, desde que, sejam plenamente capazes ou a causa possa ser resolvida por autocomposição (art. 471). Segundo o Desembargador Brant (2013), a justiça deve nomear o perito revestido de total imparcialidade e isenção, "não sendo admitida qualquer intervenção ou indicação por qualquer das partes, sob pena de se ferir o contraditório e ampla defesa, revelando-se claro cerceamento de defesa".

2.5.1. Diferença entre *e-Discovery* e a forense digital

De todos os princípios de forense digital citados por Casey (2009), apenas um deles é passível de contestação no processo de *e-Discovery*, o princípio da objetividade. Enquanto na forense digital os investigadores não tem ideia, em teoria, do que será concluído, buscando interpretar as evidências sem qualquer tipo de preconceito, no *e-Discovery*, os responsáveis pela investigação sabem exatamente as informações de que eles necessitam e de que forma devem utilizá-las.

A chave para diferenciar *e-Discovery* e forense digital se encontra no fato que na forense digital os peritos se preocupam em encontrar evidências incriminatórias ou absolutórias em um processo judicial. O perito se atém ao papel para o qual foi designado, atuando de forma isenta, como analista ou assessor técnico (CASEY, 2009). No *e-Discovery*, a empresa solicita a outra empresa informações pertinentes à sua tese em uma ação judicial.

Ademais, no *e-Discovery*, o maior desafio envolve tanto o campo jurídico como o campo da tecnologia da informação - TI. Ambos os lados precisam conhecer e se familiarizar com os termos e questões da informática, assim como da área do Direito. Muitos casos judiciais são perdidos porque os juízes e advogados desconhecem as terminologias da TI, como também o contrário acontece, alguns peritos em informática não entendem os procedimentos legais.

(PHILLIPS et. al., 2013). A Figura 2.4 ilustra duas perspectivas entre forense digital e *e-Discovery*.

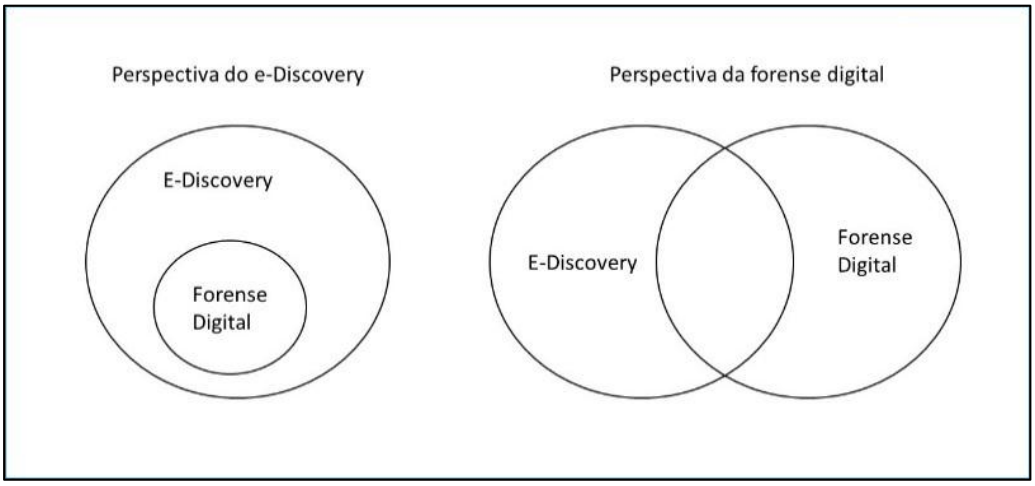

Figura 2.4 - O relacionamento entre e-Discovery e forense digital (Phillips et al., 2013, tradução)

Observa-se que, na perspectiva do *e-Discovery*, a forense digital está contida dentro do conjunto *e-Discovery*, por entender que a forense digital é apenas uma parte de um todo do processo de *e-Discovery*. No entanto, enxergando pela perspectiva da forense digital, o *e-Discovery* compartilha de pontos comuns com a forense digital, mas possuem atribuições distintas, conforme supracitado.

Neste trabalho, adota-se a visão de que a perspectiva da forense digital é a mais adequada: embora ambos compartilhem da maioria dos princípios da forense digital, existem divergências no que tange ao objetivo final, um trabalha numa situação de imparcialidade e imprevisibilidade da conclusão, que é o caso da forense digital, enquanto o outro, ao contrário, já é parcial e previsível, pois já tem ideias das evidências que deseja encontrar com o objetivo de provar uma tese.

2.6. DIREITO DIGITAL

A advogada especialista, Patricia Peck Pinheiro (2010) trabalha com a seguinte definição de Direito Digital:

> O Direito Digital consiste na evolução do próprio Direito, abrangendo todos os princípios fundamentais e institutos que estão vigentes e são aplicadas até hoje, assim como introduzindo novos institutos e elementos para o pensamento jurídico, em todas

> as suas áreas (Direito Civil, Direito Autoral, Direito Comercial, Direito Contratual, Direito Econômico, Direito Financeiro, Direito Tributário, Direito Penal, Direito Internacional, etc.)

Segundo Pinheiro (2012) o Direito Digital possui um elemento a mais em sua visão tridimensional (fato, valor e norma), o elemento tempo. A Justiça precisa agir de forma rápida para materializar o próprio Direito. Uma justiça lenta é um fator de exclusão. Em determinados casos, para uma resposta que necessite de decisões rápidas a um dano real, o fator tempo será determinante para um pedido ao judiciário.

Conforme Hoeschl (2003), o direito digital tem duas noções, uma de caráter substantivo e outra de caráter adjetivo:

> A primeira define o direito referente à vida digital. A segunda refere-se ao o direito que está em bits. O primeiro sentido diz respeito ao aspecto substantivo da ciência jurídica. Assim como o direito comercial trata das questões relativas ao comércio, assim como o direito criminal trata das questões referentes aos crimes, e o direito constitucional refere-se à Constituição e à teoria constitucional, o direito digital agrupa as questões referentes à vida digital. É o direito dos bits. O segundo significado refere-se aos atributos e características de certos tipos de normas e comandos jurídicos, aqueles formulados, materializados e consolidados em ambientes digitais. É o direito que está em bits. Sua evolução - em ambos os aspectos - é vital para a ciência jurídica do futuro, bem como para a organização social.

Em abril de 2006, a Suprema Corte Americana determinou alteração no Código de Processo Civil Federal (*Federal Rules of Civil Procedure - FRCP*) para incluir a questão do *e-Discovery*. As alterações realizadas obrigaram as empresas a proteger os seus dados para disponibilidade em caso de um processo de *discovery* (descoberta), como forma de antecipação de um possível litígio. Além do FRCP, nos Estados Unidos, existem o Código de Processo Criminal Federal (*Federal Rules of Criminal Procedure - FRCrP*) e o Código Federal de Evidência (*Federal Rules of Evidence - FRE*) que tratam de questões relacionadas ao *e-Discovery*. (PHILLIPS et. al., 2013).

Em 2007, um grupo de advogados americanos, em parceria com outros profissionais que lidam com documentos eletrônicos, apresentaram em uma conferência os princípios de "Sedona". Esses princípios funcionam como um manual básico para tratamento de *e-Discovery*. Ao todo são 14 princípios, sendo que o primeiro princípio trata da obrigação das empresas de preservarem o ESI relevantes para fins de antecipação de um litígio. (PHILLIPS et. al., 2013).

No Brasil, o assunto *e-Discovery* não é tema de uma legislação específica e não existe qualquer tipo de princípio para tratar de informações eletrônicas armazenadas, como os Princípios de Sedona, mesmo porque o termo *e-Discovery* é pouco conhecido no meio jurídico e governamental, como também são poucos os especialistas de informática brasileiros que conhecem sobre o assunto.

É possível verificar um processo de evolução da nossa legislação em termos de leis que tem o caráter de robustecer o que se pode dizer de Direito Digital Brasileiro. A lei nº 9.296, de 24 de julho de 1996, é um exemplo de lei que trata da interceptação de comunicações telefônicas, de qualquer natureza, como também da interceptação do fluxo de comunicações em sistemas de informática e telemática para prova em investigação criminal e em instrução processual penal.

Conhecida como Lei Carolina Dieckmann, a Lei 12.737, 30 de novembro de 2012, dispõe a tipificação penal de delitos de informática. Essa lei entrou em vigor e em 2 de abril de 2013 e inseriu no Código Penal brasileiro os arts. 154-A e 154-B, no art. 266 do diploma legal inseriu dois parágrafos e, na redação do art. 298 do Estatuto Penal em vigor, o parágrafo único. (REIS, 2015).

Para Reis (2015) houve um avanço da legislação brasileira em tipificar crimes cibernéticos:

> Notório que a legislação brasileira era ineficiente para penalizar as condutas praticadas através de dispositivos de informática, daí o advento da Lei nº 12.737/12, que passou a coibir, na seara penal, a prática de infrações cometidas em ambiente virtual.

Ainda se tratando do mesmo contexto e que também entrou em vigor na mesma data da Lei Carolina Dieckmann, a Lei nº 12.735, de 30 de novembro de 2012, reconhecida como Lei Azeredo, tipificou as condutas realizadas mediante uso de sistema eletrônico, digital ou similares, praticadas contra sistemas informatizados e similares.

> Art. 4º Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.

De acordo com Pinheiro e Haikal (2013) ambas as leis 12.735 e 12.737, não tipificam todo arcabouço de delitos penais digitais, mesmo porque o direito digital evolui no mesmo sentido do desenvolvimento tecnológico, novos regramentos serão necessários para coibir práticas ilícitas que ainda hão de surgir.

> (...) não esgotaram os tipos penais digitais pois é impossível que não se considere como crime a indisponibilidade de sistemas de informação de entidades privadas, como sites de comércio eletrônico ou bancos, ou a disseminação de vírus e outros códigos maliciosos, em razão da sociedade inteira estar cada vez mais interconectada. Pinheiro e Haikal (2013).

A publicação da Lei nº 12.965, de 23 de abril de 2014, conhecida como popularmente o Marco Civil da Internet ou a Constituição da Internet Brasileira, estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Essa lei garante diversos direitos como privacidade dos usuários, liberdade de expressão, neutralidade da rede, e também pontos

importantes e que são pertinentes ao processo *e-Discovery*, como a guarda de logs de conexão e de acesso às aplicações.

> Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento. (Brasil, 2014)
> (....)
> Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento. (Brasil, 2014).

Apesar do tempo de retenção de logs de conexão e de acesso às aplicações não se estenderem ao Poder Público no que diz respeito ao Marco Civil da Internet, mesmo assim, os órgãos públicos estão sujeitos a prestarem informações ao Poder Judiciário, aos Órgãos de Controle Interno e Externo e principalmente à sociedade quando acionados. Por isso é salutar que a Administração Pública esteja preparada para enfrentar um processo de *e-Discovery*, mesmo sendo um termo ainda pouco conhecido no Brasil.

Atualmente, com a regulamentação do direito constitucional de acesso às informações, Lei nº 12.527/2011, conhecida como Lei de Acesso à Informação – LAI, "todas as informações produzidas ou sob guarda do poder público são públicas e, portanto, acessíveis a todos os cidadãos, ressalvadas as informações pessoais e as hipóteses de sigilo legalmente estabelecidas" (Brasil, 2016).

De acordo com a Norma Complementar nº 20/IN01/DSIC/GSIPR, publicada no Diário Oficial da União – DOU, no dia 15 de dezembro de 2014, os órgãos e entidades da Administração Pública Federal – APF devem realizar o adequado tratamento da informação no decorrer das fases do ciclo de vida e ressalva a necessidade por parte dos agentes públicos em observar os dispositivos estabelecidos na legislação relativa a temas como Segurança da Informação e Comunicações – SIC, gestão documental e arquivística, gestão da informação, acesso à informação, e sigilo da Informação.

> 4.4 A informação institucional dos órgãos e entidades da APF deve ser tratada visando as suas funções administrativas, informativas, probatórias e comunicativas, e considerados os princípios de acesso a informação dispostos pela Lei nº 12.527/2011 e seus Decretos nº 7.724/2012 e nº 7.845/2012.
> 4.5 É dever do agente público salvaguardar a informação sigilosa e a pessoal, bem como assegurar a publicidade da informação ostensiva, utilizando-as, exclusivamente, para o exercício das atribuições de cargo, emprego ou função pública, sob pena de responsabilização administrativa, civil e penal. (BRASIL, 2014).

De acordo com a LAI (BRASIL, 2014), os órgãos e entidades públicas devem divulgar em local de fácil acesso informações de interesse coletivo ou geral por eles produzidas ou

custodiadas e para cumprimento do disposto é obrigatória a divulgação em sítios oficiais da rede mundial de computadores – internet. Esses sítios devem atender a determinados requisitos, dos quais dois são destacados a seguir:

> II - possibilitar a gravação de relatórios em diversos formatos eletrônicos, inclusive abertos e não proprietários, tais como planilhas e texto, de modo a facilitar a análise das informações;
> III - possibilitar o acesso automatizado por sistemas externos em formatos abertos, estruturados e legíveis por máquina;

Destaca-se dos requisitos supracitados que o formato[17] deve ser aberto, o que favorece uma política de Dados Abertos Governamentais[18].

Segundo o Portal Brasileiro de Dados Abertos (http://dados.gov.br/) um dos princípios para se trabalhar com Dados Abertos Governamentais é o "Princípio Completos":

> Todos os dados públicos são disponibilizados. Dados são informações eletronicamente gravadas, incluindo, mas não se limitando a, documentos, bancos de dados, transcrições e gravações audiovisuais. Dados públicos são dados que não estão sujeitos a limitações válidas de privacidade, segurança ou controle de acesso, reguladas por estatutos. (BRASIL, 2016).

Esse é um ponto importante a ser observado, pois o Brasil não possui um arcabouço de regras específicas para tratamento de *e-Discovery*, no entanto existem leis que podem apoiar o trabalho de descoberta eletrônica para atendimento de demandas diversas, seja da sociedade, seja do judiciário. Se a Administração Pública produz informações públicas, então, essas informações devem ser disponibilizadas em formato aberto como forma de proporcionar transparência a gestão pública, respeitando obviamente, o caráter sigiloso de determinadas informações. De certa forma, se os órgãos da APF simplesmente atenderem aos dispositivos legais referentes ao tratamento da informação, já seria um passo essencial para o processo de *e-Discovery*.

Outro avanço da legislação brasileira em matéria de Direito Digital, é o Projeto de Lei do Senado (PLS) nº 330/2013, que cria um marco regulatório para a proteção, o tratamento e o uso dos dados pessoais dos brasileiros. O Marco Regulatório tem como objetivo regulamentar a proteção, o tratamento e o uso de dados das pessoas naturais e jurídicas de direito público ou privado. Define também os casos em que os dados considerados sensíveis poderão ser coletados, armazenados, processados, transmitidos, utilizados, fornecidos a usuários ou divulgados. (BRASIL, 2016).

---

[17] Dados em formato aberto - dados representados em meio digital em um formato sobre o qual nenhuma organização tenha controle exclusivo, passíveis de utilização por qualquer pessoa (BRASIL, 2016)
[18] Dados são abertos quando qualquer pessoa pode livremente usá-los, reutilizá-los e redistribuí-los, estando sujeito a, no máximo, a exigência de creditar a sua autoria e compartilhar pela mesma licença (BRASIL, 2016).

"O texto estabelece que os dados pessoais não poderão ser utilizados para prejudicar o cidadão. A coleta deve ser feita sob consentimento, assim como o armazenamento e o tratamento dados às informações pessoais". (BRASIL, 2016).

> Uma vez aprovada, a lei será aplicada mesmo que a atividade seja realizada por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos um integrante do mesmo grupo econômico possua estabelecimento no Brasil. Da mesma forma, se a coleta, armazenamento ou utilização dos dados pessoais ocorrer em local onde seja aplicável a lei brasileira por força de tratado ou convenção. (BRASIL, 2016).

E o que se pode chamar de um provável *e-Discovery* brasileiro é que ele será útil e necessário para examinar uma grande quantidade de informações que estará disponível para fins de conformidade legal. Consequentemente, o Poder Judiciário poderá inquirir que qualquer empresa ou órgão público apresente seus dados eletrônicos para tratamento de processos litigiosos. É certo que no mundo tecnológico de hoje não é uma questão saber se a empresa ou órgão acabará em um litígio; mas é a questão de quando.

2.7. CONSIDERAÇÕES

As considerações a seguir apresentam um breve resumo da base conceitual tratada neste capítulo:

- *e-Discovery* pode ser compreendido como um processo que se utiliza de informações em meio digitais para produção de provas ou evidências eletrônicas relevantes em uma disputa judicial;
- O conceito de evidência eletrônica como sendo informações armazenadas eletronicamente ou digitalmente, em inglês, *Eletronically Stored Inf*ormation – ESI. Essas informações podem estar apostas em documentos, sistemas operacionais, e-mails, fotografias digitais, figuras, páginas em sítios da Internet, memórias dos celulares, em discos rígidos, em mídias flexíveis como DVD´s e CD´s, etc;
- A maturidade em governança de TI colabora com os eventuais requisitos presentes nas fases para descoberta eletrônica do processo de *e-Discovery*. Quanto maior a maturidade em governança de TI de uma organização melhores serão as possibilidades de se obter resultados satisfatórios do *e-Discovery*;
- Na forense digital os investigadores não têm ideia, em teoria, do que será concluído do caso, buscando interpretar as evidências sem qualquer tipo de preconceito. No *e-Discovery*, os responsáveis pela investigação sabem

exatamente as informações que eles necessitam e de que forma devem utilizá-las em seus processos judiciais; e

- Nos Estados Unidos tem-se aplicado os princípios de “Sedona” como um manual básico para tratamento de *e-Discovery*. Ao todo são 14 princípios, sendo que o primeiro princípio trata da obrigação das empresas de preservarem o ESI relevante para fins de antecipação de um litígio. No Brasil, o assunto *e-Discovery* não é tema de uma legislação específica, mas existem iniciativas que dão respaldo para preservação de algumas informações armazenadas eletronicamente.

3. MÉTODOS E MODELOS RELACIONADOS AO E-DISCOVERY

Um dos grandes desafios para profissionais de TI que atuam em casos que envolvam *e-Discovery* é aprender a ler e entender os termos e os processos judiciais. Muita da legislação americana que se refere a *e-Discovery* e a forense digital é nova e necessita de interpretação e desenvolvimento. Uma das formas de se aprender como proceder em casos de *e-Discovery* é a princípio realizar consultas às jurisprudências que sejam mais recentes. Tem-se a noção que os profissionais de TI são apenas os executores do processo e que os profissionais do direito são os intérpretes das questões legais. Entretanto, a TI precisa aprender a lidar com as questões legais para determinar quais são os pontos importantes e relevantes em casos de *e-Discovery*. (PHILLIPS et. al., 2013).

Este capítulo aborda método e modelos relacionados ao *e-Discovery.* Na seção 3.1 é apresentado o método FIRAC, um método simples que pode auxiliar profissionais de TI a compreender o que se trata um determinado caso judicial e na seção 3.2 o modelo EDRM para tratamento do processo de *e-Discovery*.

3.1. MÉTODO FIRAC

O método FIRAC (*Facts, Issues, Rules and References, Analysis and Conclusions*) é uma derivação do termo IRAC, que é uma ferramenta básica para leitura, análise e escrita de casos judiciais pelos estudantes americanos da faculdade de direito. Esse método também pode ser utilizado por profissionais de TI a fim de ganhar conhecimento de contexto do que irão trabalhar durante as fases subsequentes do *e-Discovery*. De certa forma, é um método que ajuda a comunicação entre o mundo jurídico e tecnológico. Phillips adiciona a letra F ao termo IRAC para relacioná-lo aos fatos, questões, regramentos e referências, análise e conclusões de um caso. Quando se faz a leitura de um caso, os fatos se referem a quem, o que, quando, onde e como isso veio a acontecer. E surge a questão por que o autor entrou com uma ação judicial.

O uso do método FIRAC é bastante simples e pode ser implementado por meio de ferramentas que fazem uso da funcionalidade de realce do editor de texto à medida que vão sendo encontradas informações relevantes na leitura ou na revisão do caso. Por exemplo, os fatos podem receber um realce de cor verde (indicando o início de um caso) e as conclusões podem ser realçadas de vermelho (indicando o fim de um caso). (PHILLIPS et. al., 2013).

A Figura 3.1 descreve o que cada letra significa e quais as perguntas que deverão ser realizadas para que se encontrem as devidas respostas. Ao final do processo de coleta de

informações sobre o caso, o profissional de TI terá melhores condições de colaborar na descoberta de evidências eletrônicas.

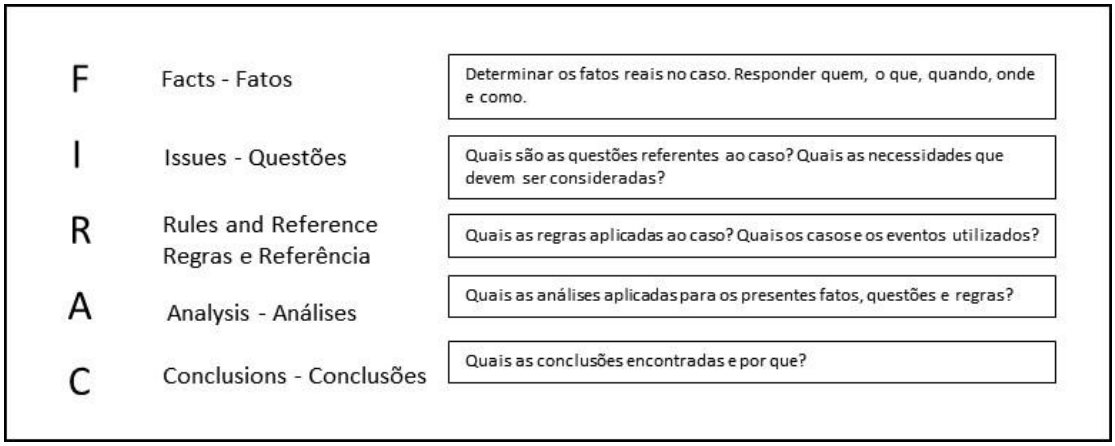

Figura 3.1 - O Método FIRAC (PHILLIPS et. al., 2013, tradução)

3.2. MODELO EDRM

O modelo de referência para descoberta eletrônica (*Eletronic Discovery Reference Model - EDRM*) teve o seu conceito descrito por George Socha e Tom Gelbmann. O modelo de referência divide o processo de *e-Discovery* em seis fases, que podem se desdobrar em uma ou mais etapas (Newton e Johnson, 2014), a saber:

- Governança da Informação: normas, diretrizes, processos, políticas e responsabilização na avaliação, criação, armazenamento, uso, arquivamento e eliminação da informação, para permitir que uma organização atinja os seus objetivos de negócio.
- Identificação: identifica potenciais fontes de informações armazenadas eletronicamente.
- Preservação/Coleta: assegura que as informações armazenadas eletronicamente estão protegidas contra alterações inapropriadas ou destruição, a fim de que sejam coletadas para uso em processos judiciais.
- Processamento/Revisão/Análise: o processamento serve para reduzir o quantitativo de informações coletadas e converter as informações em um formato apropriado. A revisão contribui para avaliar as informações que são relevantes e sensíveis. A análise avalia o conteúdo e o contexto das informações relevantes.

- Produção: preparação das informações armazenadas eletronicamente em mídia para serem submetidas ao processo judicial.
- Apresentação: exposição das informações armazenadas eletronicamente no formato estabelecido entre as partes para validar os fatos ou posicionamento ou, ainda, para persuadir a audiência.

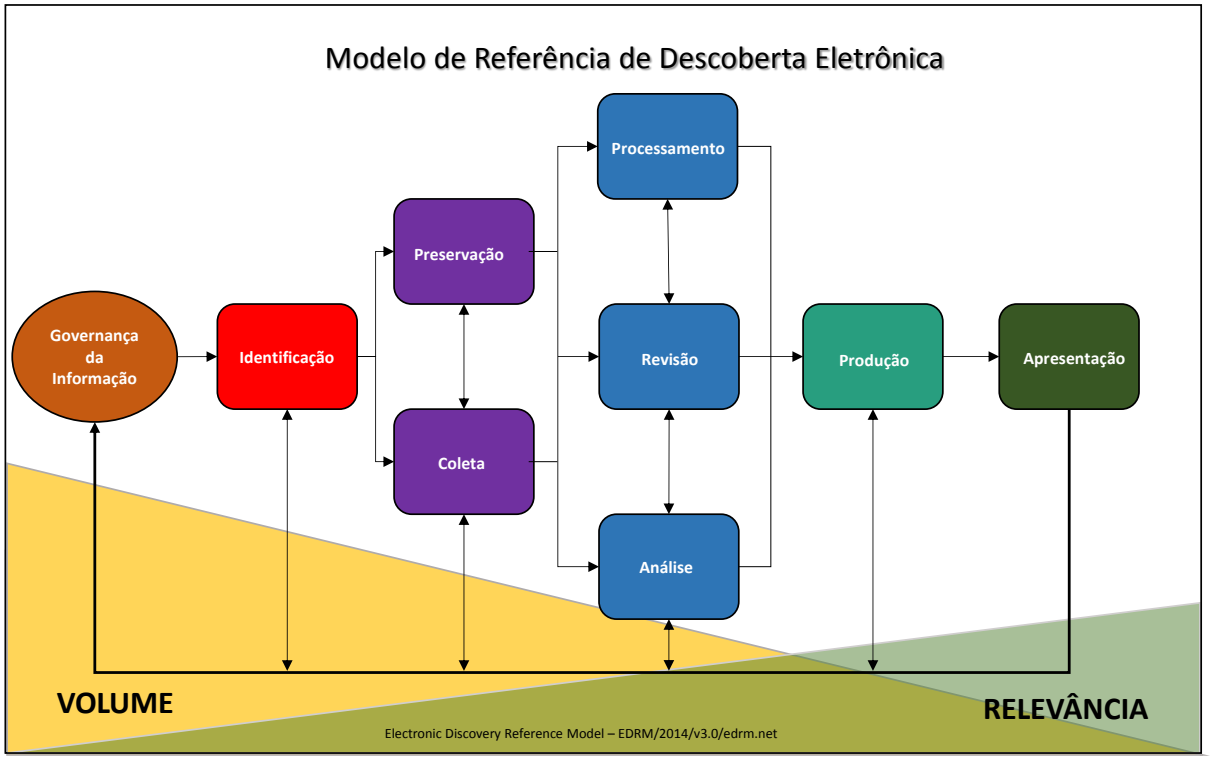

Figura 3.2 - Modelo de Referência de Descoberta Eletrônica (EDRM, 2014, tradução)

O diagrama EDRM não é um modelo em cascata e nem deve ser trabalhado de forma linear, pode envolver algumas etapas, mas não necessariamente todas as etapas delineadas no diagrama, alguns passos podem ser executados em ordem diferente do mostrado. De acordo com a Figura 3.2 no início das fases do EDRM tem-se um grande volume de informações a serem identificadas, preservadas e coletadas, à medida que essas informações se submetem as fases de processamento, revisão e análise, o volume de dados diminui e aumenta relevância das informações produzidas e que servirão como provas e evidências perante a Justiça.

Ademais, o diagrama EDRM representa uma visão conceitual do processo de *e-Discovery*, é na verdade, um processo iterativo. Podem-se repetir os mesmos passos várias vezes até que se consiga um resultado desejado. É possível que seja necessário executar novamente etapas realizadas anteriormente, refinando sua abordagem para uma melhor compreensão dos dados

apresentados. Ele serve como uma base para discussão e análise, e não deve ser encarado como uma única forma de abordar *e-Discovery.* (EDRM).

Por isso o modelo é muito útil, mesmo para quem não tem muita experiência em *e-Discovery*, serve como um guia para um processo de identificação de dados e subsequentemente para preservação destes dados, coletas e processamento. (Newton & Johnson, 2014).

Nos Estados Unidos o EDRM serve como uma orientação para lidar com situações de litígios, também é muito utilizado no meio empresarial. O modelo possibilita tratar uma grande quantidade de informações e reduzi-la àquelas que são realmente essenciais para o caso. (PHILLIPS et. al., 2013).

As próximas subseções detalham as etapas do EDRM, conforme descrito pelo modelo gerenciado pela *Duke Law Center for Judicial Studies* da Universidade de Duke em Durham, NC, Estados Unidos da América (Duke Law, 2016). O *e-Discovery* e o EDRM adotam uma nomenclatura própria que, em alguns casos, pode conflitar com o uso de termos em outras áreas. Neste trabalho buscou-se o alinhamento à nomenclatura conforme descrito no glossário do EDRM. (EDRM, 2016).

3.2.1. IGRM

Durante o processo de desenvolvimento do modelo EDRM, algumas empresas participantes sentiram a necessidade de criar um modelo próprio para o Modelo de Referência para a Governança da Informação (*Information Governance Reference Model – IGRM*) (PHILLIPS et. al., 2013), conforme apresentado na Figura 3.3:

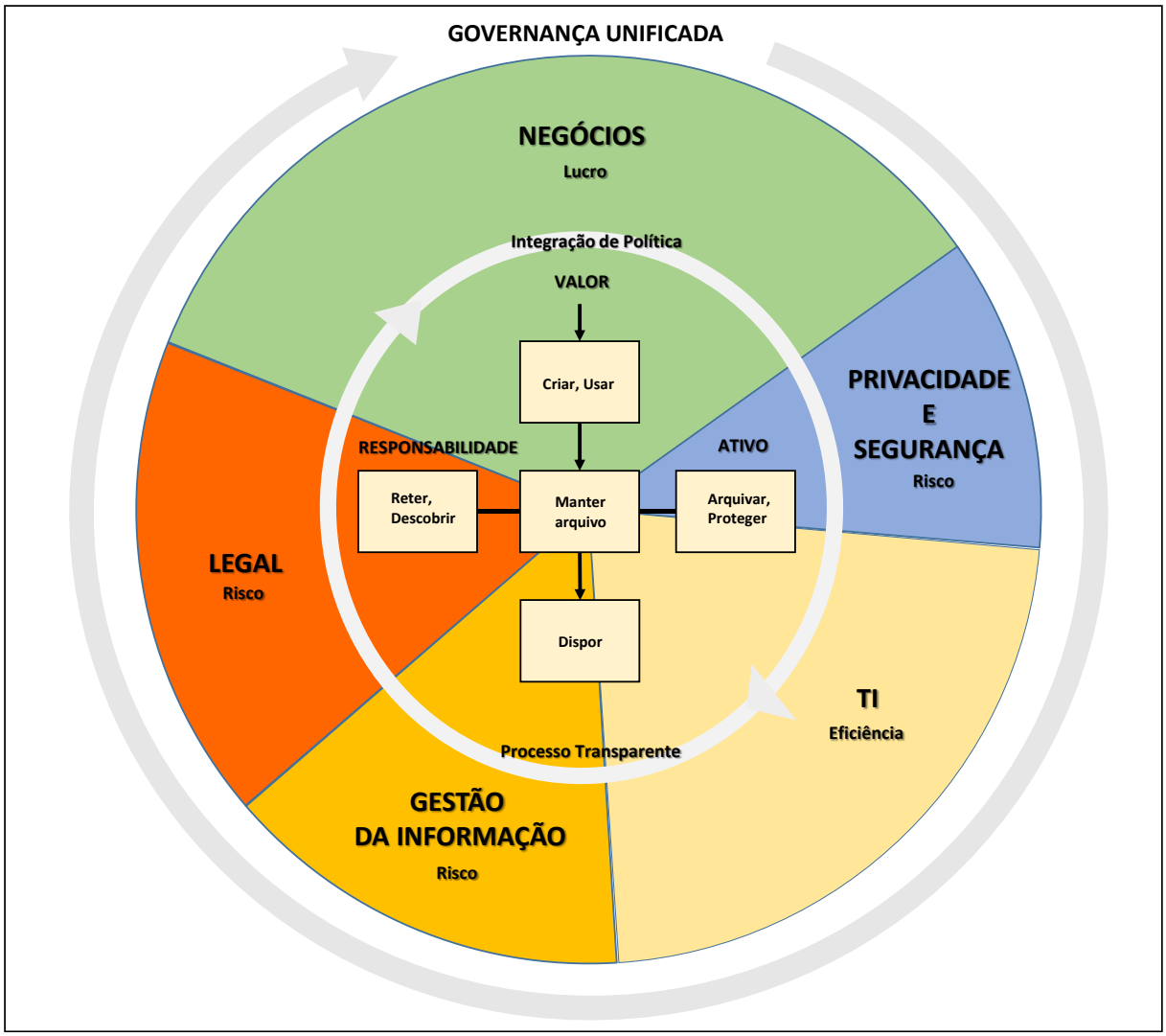

Figura 3.3 - Modelo de Referência da Governança da Informação (EDRM, 2012, tradução)

Segundo Socha (2012, *apud* LEDERGEBER & KNOUFF) o IGRM é uma poderosa ferramenta de comunicação que os advogados podem utilizar como orientação à liderança e às principais partes interessadas da organização. A intenção é facilitar o diálogo entre as partes interessadas e a organização, provendo uma linguagem comum entre ambos os lados para suporte à tomada de decisões. (EDRM). A Governança da Informação impacta no *e-Discovery* e na conformidade.

Mais formalmente, o Gartner (2012, *apud* LEDERGEBER & KNOUFF) define Governança da Informação como o direito de tomada decisões e responsabilização quanto às ações de validação, criação, armazenamento, uso, arquivamento e deleção da informação.

Para Ledergerber (2012, *apud* EDRM) governança da informação é um processo de negócio que tem como objetivo reduzir os riscos e aumentar a eficiência por meio da melhoria

dos processos. “O *e-Discovery* estará cada vez mais integrada à política de governança da informação, aos procedimentos e à infraestrutura de uma organização”.

O objetivo do modelo IGRM, portanto, é o de prover uma estrutura comum, prática e flexível para o desenvolvimento da eficácia de programas que gerenciam informações. O modelo IGRM envolve diversos setores, jurídico, tecnologia da informação, partes interessadas, gerência das organizações.

3.2.2. Identificação

A identificação deve ser tão completa e abrangente quanto possível. Nessa fase a equipe de identificação executará um plano para identificar e validar informações eletrônicas relevantes, incluindo pessoas e sistemas.

Algumas unidades da organização provavelmente serão envolvidas nessa fase, como a gerência, setor de contratos, os recursos humanos – RH, área de TI (redes, sistemas, backup, etc). O objetivo é identificar os locais onde estão esses recursos e indicá-los para a realização de uma possível coleta de dados.

A equipe de identificação pode conduzir entrevistas com as pessoas envolvidas no processo judicial para determinar os tipos de informações que serão relevantes. Entrevistas com a equipe de TI, principalmente a equipe de redes, para determinar como são armazenadas as informações, verificar a política e o processo de backup.

Pode ser que no decorrer do processo judicial ocorram mudanças à medida que o litígio progride. Para isso é importante que a equipe de identificação esteja atenta quanto à entrada de novas informações que contribuam para o processo. O escopo de informações sujeitas a preservação e a divulgação é, portanto, dinâmico. Identificação requer diligência, investigação e pensamento analítico.

Conforme demonstrado na Figura 3.4, identificar a origem dessas informações relevantes passa por 4 (quatro) fases: desenvolver um plano e a estratégia de identificação; estabelecer uma equipe de identificação; identificar fontes de ESI potencialmente relevantes e certificar fontes de ESI relevantes.

O foco, a princípio, será o meio digital, embora existam informações pertinentes que possam estar em papel.

As próximas seções descrevem as etapas descritas na Figura 3.4.

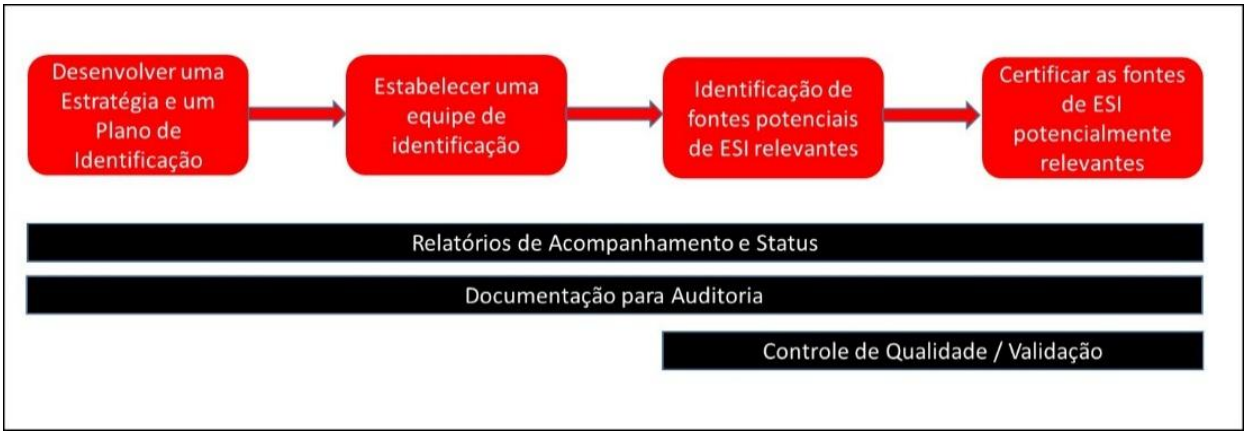

Figura 3.4 - Fluxo para Identificação de ESI (EDRM, 2010, tradução)

3.2.2.1. Desenvolver uma estratégia e um plano de identificação

A estratégia e o plano de identificação podem seguir duas frentes, uma delas é identificar as partes envolvidas, os custodiantes, a localização e a rastreabilidade dos dados individuais e coletivos. A outra frente é identificar as pessoas envolvidas no gerenciamento de projetos, os juristas, a equipe da TI, prestadores de serviços, etc. A estratégia e o plano de identificação podem colaborar com o apontamento da equipe que deve estar envolvida com a identificação de fontes relevantes de ESI.

A organização deve tomar as medidas necessárias para identificar e preservar as informações ESI quando essas forem importantes para uma investigação ou litígio, podendo ser realizado até mesmo de forma preventiva. Adotar protocolos para elaboração de normativos e regulamentos são ações que também contribuem para o processo de *e-Discovery* e para a governança de TI.

Outro fator de suma importância é a identificação dos sistemas críticos, principalmente os sistemas que não estão hospedados em uma plataforma de rede e que são de uso individual. Esses sistemas também são passíveis de preservação de dados, investigação e litígio. A proatividade, quanto à coleta de informações em momento oportuno em sistemas de alto risco, facilita o trabalho das organizações e também dos tribunais. Por isso a necessidade também de a organização saber quem são os gestores desses sistemas. (EDRM).

Antes de elaborar um plano, a equipe responsável pelo *e-Discovery* necessita fazer o mapeamento de dados inicial, que será descrito a seguir.

Mapeamento de dados

De acordo com o modelo de EDRM, *"não pode proteger aquilo que não sabe que existe"*. Essa máxima vem de encontro com a necessidade das organizações de mapear suas fontes de informações. Isso é um fator de sucesso para o processo de *e-Discovery*. Cada organização possui uma infraestrutura própria de TI e que se difere uma das outras, os sistemas de gerenciamento de usuários e ativos de TI, o de e-mails e de backup, principalmente quando a organização possui filiais em diferentes pontos geográficos.

O processo de identificação de sistemas envolve os diferentes tipos de servidores instalados na organização, servidores de e-mails, de arquivos, de sistemas (backup) que de certa forma estão inter-relacionados e são monitorados pela equipe de TI. Além dos servidores instalados em um provável *Data Center* ou em uma sala segura, existem também os diversos tipos de microcomputadores, impressoras, notebooks, dispositivos móveis (telefones inteligentes, *tablets*, cartões de memória, etc.) utilizados pelos usuários de TI da organização.

Outra questão que deve ser levada em consideração é o tipo de tratamento que a organização realiza em relação às informações que não são mais utilizadas, em seus diversos meios: discos rígidos, fitas de backups antigas, pen drives; descarte de microcomputadores, notebooks, servidores, e equipamentos de TI obsoletos e versionamento de softwares e sistemas para acesso aos dados legados.

Preparar um plano de investigação

Uma vez realizado o mapeamento de dados, o Plano de Identificação define as atividades e as ferramentas que deverão ser utilizadas para levantamento das fontes de ESI potencialmente relevantes. Esse plano pode apoiar a identificação de informações para cumprimento de ordens judiciais, como também apoiar o tratamento da segurança da informação da própria instituição.

A seguir são apresentados os fatores necessários para a elaboração de um Plano de Investigação:

- Disponibilidade de ferramentas que apoiem na identificação de pessoas e custodiantes de dados que são detentores de informações potencialmente relevantes;
- Conhecimento das áreas relacionadas, palavras-chaves e a quantidade de dados;
- Procedimentos que vinculam informações aos seus custodiantes;

- Habilidade para realizar pesquisas com palavras-chave e utilização de filtros;
- Disponibilidade de mapeamento de dados e o conhecimento dos sistemas que contêm as informações eletronicamente armazenadas – ESI.

O plano deverá garantir que todos os bancos de dados foram mapeados, além de apresentar quem são as pessoas que estão como custodiantes dessas informações. O plano é um documento vivo que pode ser alterado com o andamento dos trabalhos, pois novas informações podem ser acrescentadas ou suprimidas no decorrer do processo.

O plano deve constar informações de lotação da pessoa ou do custodiante, cargo, que tipo de informação é de sua responsabilidade (sistema, contrato específico, projeto, etc.).

Deve-se elaborar uma lista inicial com os nomes das pessoas que detêm o conhecimento de informações relevantes dentro da organização. Caso existam pessoas que não estejam lotadas na área de TI que são detentoras desse tipo de informação, elas também devem ter seus nomes mencionados nessa lista, o que engloba as pessoas das áreas meio e fim da organização. Elaborar uma lista servirá de base para uma futura consulta das áreas custodiantes de informações relevantes dentro da organização.

Uma vez produzida uma lista inicial com nome de pessoas que podem apontar informações relevantes para o processo, é importante compreender se a pessoa é custodiante e responsável pelas informações ou se a pessoa pode apenas colaborar com a localização dos dados, não sendo responsável pelas informações. Esta definição contribui para selecionar os tipos de perguntas que serão apropriadas para cada tipo de indivíduo. Para os custodiantes facilita a identificação das informações que são chaves e aquelas que não são e também contribui para identificar os tipos de registros que provavelmente estão sobre a sua guarda. A abordagem a ser tomada vai depender desses fatores.

Após a elaboração da lista, deve-se verificar como se planeja identificar as informações necessárias, se todos serão entrevistados ou se será utilizada uma pesquisa para pessoas que não são importantes no processo. Às vezes pode ocorrer de se preparar uma pesquisa e alterar uma entrevista dependendo do caso e da situação. O ideal é que se tenha um modelo de entrevista e de pesquisa a ser aplicado.

3.2.2.2. Estabelecer uma equipe de identificação

A equipe de identificação é responsável pelo Plano de Identificação. Essa equipe tem a responsabilidade de identificar os dados relevantes, os dados dos custodiantes e as pessoas chaves do processo. A equipe deve conter um ou mais representantes das seguintes áreas:

- Consultoria Jurídica da Organização – responsável por elaborar o plano de resposta do *e-Discovery* que inclui um plano de identificação e as possíveis áreas e sistemas que possuem informações relevantes que poderão ser utilizadas para pedidos judiciais para fins de retenção de informações.
- Consultoria jurídica externa[19] – deve entender o plano de identificação e assegurar que seja viável.
- Analista de TI - responsável em identificar e levantar informações relevantes em hardware e software.
- Equipe de Infraestrutura de Redes – equipe responsável pelo armazenamento de dados na rede e da política de backup.
- Custodiantes de informações (área de negócio / TI) – informa os sistemas que contém informações relevantes e onde estão armazenadas essas informações.
- Recursos Humanos – providenciam uma lista com os nomes dos funcionários, as suas atribuições, cargos, etc, com a finalidade de identificar potenciais custodiantes.
- Liderança – identifica os sistemas utilizados pelas áreas de negócios e pessoas chaves que detenham conhecimento de um determinado tipo de informação que seja relevante.
- Provedores de serviços e consultores de *e-Discovery* – oferecem o conhecimento técnico e pericial para identificar a localização de informações relevantes.

3.2.2.3. Identificação de fontes potenciais de ESI relevantes

<u>Identificar testemunhas chaves e custodiantes</u>

Existem diversas áreas em uma organização, mas nem todas possuem informações relevantes que possam ser apresentadas em um provável litígio. Porém a coordenação de TI,

[19] Nos órgãos públicos do Executivo Federal do Brasil, a Advocacia-Geral da União é a instituição que representa a União judicial e extrajudicialmente. (BRASIL, 1993).

sendo a responsável pela infraestrutura de redes e o desenvolvimento de sistemas, é a custodiante de informações de suma importância. É possível também que a outra parte interessada no processo judicial solicite determinados tipos de informações que estão de posse de uma área de negócio.

O *e-Discovery* deve ser realizado de forma que as informações coletadas tenham valia no litígio e que produzam o resultado esperado.

Geralmente, as primeiras audiências servem para que as partes do litígio entrem em entendimento sobre quais são informações necessárias para o processo de *e-Discovery*.

Determinando os prazos legais

É necessário que se reveja as peças processuais relevantes e os pedidos de *e-Discovery* para determinar o prazo para atendimento das demandas.

Lista de palavras-chave

Uma lista de palavras-chave contribui para coleta, processamento e revisão de dados. Em uma entrevista com os custodiantes de informações relevantes na organização deve-se questionar sobre o uso de jargões ou siglas utilizadas em relatórios, contratos, etc.

Identificação de documentos potencialmente relevantes e tipos de dados

Uma maneira possível de melhorar as buscas é identificando primeiramente os tipos de documentos que podem conter informações relevantes para a investigação. O importante neste caso é que as informações estejam armazenadas eletronicamente e que sejam pesquisáveis, contribuindo para o processo *de e-Discovery* para atendimento das demandas judiciais.

Exemplos de tipos de dados são os e-mails, aplicativos da Microsoft, documentos Adobe Acrobat, banco de dados, logs de acesso, aplicativos proprietários, etc. Certos tipos de dados podem ser coletados de forma indiscriminada, atendendo critérios genéricos estabelecidos em ordens judiciais.

Entrevistar os custodiantes da organização contribui para identificar informações relevantes. As entrevistas permitem acrescentar ou retirar aqueles custodiantes que serão ou não serão relevantes para identificação das informações, respectivamente.

Toda interlocução que houver entre as partes do processo deverá ser repassada à equipe de identificação para verificação de prazos, custos, produção e método de trabalho. Os acordos realizados devem seguir esta linha de tratamento para atendimento da demanda judicial.

Também é importante que a organização disponha de um calendário de atualizações de programas/sistemas e migrações de dados, que possam afetar a capacidade de utilização dos dados atualmente disponíveis ou dos dados que foram arquivados durante o curso do processo judicial.

Armazenamento de dados

A organização deve possuir um sistema de gerenciamento de documentos e de controle de documentos classificados. Os servidores específicos para armazenamento de informações devem ser listados e identificados, de preferência com o nome e a versão do sistema neles instalados.

Os logs de acessos a esses servidores também devem estar disponíveis para consulta, bem como o módulo de auditoria ativado, caso haja necessidade de algum relatório de auditoria.

O conhecimento de outros critérios contribui para que a organização reveja a sua política de armazenamento, tais como:

- Existem servidores de arquivos em vários locais?
- Os dados estão armazenados no disco rígido do notebook ou no computador pessoal ou estão armazenados em pendrives, CD´s, DVD´s ou em nuvem?
- Quais os controles utilizados para gerenciar o armazenamento de dados?
- Existe uma política de descarte de discos rígidos e de computadores obsoletos?
- Existe uma política de desligamento de funcionários da organização?

Sistema de e-mail

O sistema de e-mail possibilita a troca de mensagem eletrônica com o meio interno e externo da organização. Os detalhes sobre hardware, sistema operacional, nome e versão do software, localização de servidores e os responsáveis pelo correio eletrônico são importantes para controle e administração desse sistema.

Cabe também verificar em que tipos de servidores está instalado o sistema de e-mail e o local onde estão esses servidores. Além do mais, é importante que a organização detenha o conhecimento referente aos procedimentos de criação e exclusão de caixa de e-mail, política de

retenção, restrição de envio, tamanho da caixa, criptografia, acesso remoto, políticas de backup de caixa de e-mails. Enfim, uma série de critérios que precisam ser levados em consideração, uma vez que interferem na segurança da informação na comunicação.

Determinar a relevância da política de backup, de descarte e o Sistema de Recuperação de desastre

O backup tem como princípio a recuperação das informações em caso de um evento catastrófico ou de um desastre. A sua finalidade é a recuperação não somente de um simples e-mail ou arquivo, mas também do todo ou parte de um sistema.

As fitas de backup são um tipo comum de armazenamento, pois tem elevada capacidade de armazenamento de informações por um custo relativamente baixo. As fitas também podem ser disponibilizadas em um lugar diferente da localização da empresa ou organização.

Existem variados tipos de sistemas de backup e cada empresa deve adquirir um que se adeque à sua realidade, mas o primordial é que, em caso de necessidade, seja em razão de um desastre ou de um erro operacional, a organização tenha condições de fazer uso real do seu sistema de backup para recuperação das informações que foram perdidas ou deletadas.

A equipe de tecnologia da informação tem um papel essencial quanto ao fornecimento dos detalhes sobre o procedimento de backup e à execução de sua política. Tarefas como uma lista de checagem de realização de backup, temporalidade, local de armazenamento, sistemas e servidores agendados para o processo de backup possibilitam um controle e conhecimento da equipe de TI para casos de necessidade de recuperação de dados.

A realização de testes de restauração e recuperação de dados, antes da ocorrência de um desastre, contribui para que a empresa não se encontre desprevenida em momentos de reais necessidades. Verificar a qualidade da recuperabilidade do backup e o estado geral das mídias também devem ser levados em consideração.

E caso seja necessário o descarte das mídias que estão com defeito ou com versionamento ultrapassados, a equipe de TI tem por obrigação evitar que informações importantes da empresa sejam descartadas em um lixo qualquer sem o devido cuidado de destruição de dados sensíveis.

Sistemas Legados

Em processos de *e-Discovery*, até mesmo sistemas de versionamento anteriores devem ser levados em consideração para busca de informações relevantes para apresentação em juízo. A migração de tecnologias de hardware e software é um procedimento muitas vezes necessário para atualização e manutenção do parque tecnológico da instituição. Ocorre que isso pode levar à incompatibilidade no funcionamento de determinados sistemas. É importante que a organização realize o mapeamento desses sistemas e estabeleça uma forma de restaurar sistemas e dados de versões anteriores, caso seja necessário. Existem situações em que poucos funcionários da organização conhecem um determinado sistema e que sabem extrair as informações ali presentes. Existe sempre o risco de que esses funcionários possam um dia deixar a organização e, com isso, levar consigo conhecimento que não está documentado. Tudo isso são fatores importantes e que devem ser considerados para que sistemas se mantenham acessíveis e disponíveis para fornecimento de dados.

Computação em Nuvem ou Sistemas de Terceiros

Tem-se tornado praxe o armazenamento de informações em locais distantes da organização para fins de segurança da informação, custo-eficiência ou até mesmo para casos de recuperação de desastres. A identificação dessas fontes de armazenamento se torna necessária principalmente quando se trata de dados relevantes e que possam servir para processos judiciais. Para fins de exemplificação destes serviços, a computação em nuvem envolve SaaS[20], locação de *data centers*, terceirização de armazenamento, instalações fora da empresa, etc.

Se a organização faz uso de uma solução em nuvem, e se existem informações relevantes, será necessário na etapa de entrevista identificar onde e como estão sendo armazenadas essas informações, se existem backup dos dados, cronograma e tempo de retenção. Também é importante conhecer a política de atualização de hardware e software adotada pela prestadora desses serviços.

Em caso de os servidores de armazenamento de dados estarem localizados em outro país, será necessário conhecer a legislação pertinente para fins de coleta de informações.

[20] SaaS (Software as a Service) são basicamente os softwares que são disponíveis para os usuários através da internet (nuvem). Tais softwares são disponibilizados como serviços prestados pela empresa, onde o usuário não necessita adquirir uma licença para o uso do sistema. A principal vantagem é que o software pode ser acessado em qualquer lugar através de uma interface, como por exemplo, um navegador web. (MIZUKOSHI E GARCIA, 2015).

Fontes de Dados Adicionais

Em termos de localização física, pensar em *Data Center* como sendo o único local para armazenamento de dados da organização pode ser o mais comum, mas não é exclusivo, pois existem outras localidades que possam conter dados. Exemplos:

- Telecomunicações via "*Voice over Internet Protocol*" – VoIP[21];
- Dispositivos portáteis (ex: telefones inteligentes, tablets, pendrives, etc);
- Intranet ou extranet;
- Internet, principalmente em redes sociais;
- Notebooks e computadores pessoais;
- Virtual Private Network - VPN[22];
- Sistemas Governamentais;
- Sistemas Colaborativos (ex: Groove Technologies, SharePoint, Google Drive, Dropbox); e
- Instant Messaging – IM[23] (ex: Whatsapp, Telegram).

3.2.2.4. Certificar as fontes de ESI potencialmente relevantes

O líder da equipe de *e-Discovery* tem a responsabilidade de verificar a pertinência das fontes de ESI potencialmente relevantes para o processo judicial em questão. Os resultados encontrados não se limitam aos questionamentos, às respostas ou às objeções identificadas durante as fases do litígio. Todos os tipos de fontes ESI que foram pesquisados devem ser mencionados, a fim de demonstrar a abrangência e completude do processo de identificação.

[21] O VoIP (Voice over Internet Protocol), consiste em transmitir mensagens de voz através de uma rede usando o protocolo IP, sendo que esta é transportada sobre a forma de pacotes, ou seja, é transmitida no formato digital e não analógico. No serviço tradicional a mensagem é transportada através de uma rede de comutação de circuitos. Uma das principais razões pelas quais esta tecnologia se tornou muito popular é, devido à existência de software gratuito, pois permite dispensar os serviços de voz das companhias telefónicas, ou seja, da telefonia tradicional chamada de PSTN (*Public Switched Telephone Network*). Um outro fator importante para a popularidade desta tecnologia, é o crescimento do número de locais com acesso a banda larga. Nas chamadas tradicionais, os recursos são reservados durante a chamada e liberados no fim da mesma. Já nas chamadas VoIP, que recorre a uma infraestrutura da rede IP para a realização de chamadas, não há à priori reserva de recursos. (PEREIRA, 2015).

[22] VPN é uma sigla, em inglês, para "Rede Virtual Privada" e que, como o nome diz, funciona criando uma rede de comunicações entre computadores e outros dispositivos que têm acesso restrito a quem tem as credenciais necessárias, ou seja, é forma de criar pontes de ligação entre diferentes dispositivos via Internet, mantendo os dados de comunicação trocados entre eles codificados e mais seguros, já que sua interceptação se torna mais difícil. (GARRETT, 2015).

[23] IM é um sistema de troca de mensagens eletrônicas digitadas instantaneamente através da Internet ou de uma rede celular, utilizando uma aplicação de software compartilhado em um computador pessoal ou dispositivo móvel. (DICTIONARY, 2016).

Caso alguma fonte ESI conhecida não tenha sido pesquisada, também deve ser mencionada com as devidas justificativas pela qual não foi incluída nos resultados do processo de identificação.

O processo de certificação envolve estabelecer mecanismos de retenção de litígios[24] apropriados para o caso em questão, incluindo os recursos de hardwares, rede e sistemas.

A fase de identificação inclui a elaboração de documentos que certifique todo o processo, as ferramentas e os métodos utilizados para identificar as fontes de ESI potencialmente relevantes para possíveis questionamentos que possam surgir da parte litigante. Sem esta documentação, torna-se difícil demonstrar que o processo de identificação foi conduzido de forma correta e completa, o que pode levar à contestação pela outra parte do litígio.

3.2.2.5. Relatórios de Acompanhamento e Status

Dados o volume e complexidade das tarefas no processo de *e-Discovery*, o líder da equipe pode valer-se de relatórios de acompanhamento e status como elementos para acompanhamento das atividades executadas. Da mesma forma que os sistemas novos e manutenidos podem ser tratados como projetos, cujas partes interessadas decidirão que etapas, subetapas e detalhes devem constar no projeto, a organização pode considerar a descoberta eletrônica de um determinado caso judicial importante o bastante para ser gerenciado como um projeto, identificando riscos, dificuldades e problemas, bem como acompanhando os prazos e o orçamento relacionados.

3.2.2.6. Documentação para Auditoria

Caso haja questionamentos em relação às fontes de dados adicionais, o fato de se ter uma documentação que detalhe todo o processo de identificação possibilitará a elaboração de uma resposta em tempo hábil e mais completa possível.

A seguinte documentação poderá ser utilizada para o processo de identificação:

- Estratégia de documentação
- Plano de identificação

[24] Retenção de litígio, ou do inglês *litigation hold*, é um recurso que quando habilitado permite que todos os dados de determinado usuário em um sistema específico sejam preservados pelo tempo definido pelo administrador.

- Questões para entrevistas
- Respostas das entrevistas
- Pesquisas/Questionários
- Logs de entrevistas
- Qualquer informação que seja útil para o processo de identificação

3.2.2.7. Controle de Qualidade/Validação

A última etapa para o processo de identificação é a revisão dos passos realizados com vista a validar o que foi produzido até então em termos de completude e qualidade. Deve-se contemplar ainda as seguintes políticas:

- Política de Retenção de dados, já que alguns dados podem ser apagados ou sobrescritos.
- Política de e-mails, pois os e-mails são quase sempre alvos de busca de dados relevantes.
- Política de Backup e reciclagem de mídias.

Por último, deve ser realizado um encontro com a equipe de identificação envolvida no caso, a fim de realizar o fechamento desta etapa por meio de uma ata de reunião que registre o andamento das atividades e outras questões pertinentes.

A revisão da estratégia e do plano de identificação deve ocorrer periodicamente e caso seja necessário, um supervisor poderá ser útil para validar todos os custodiantes e documentação presentes no processo. O supervisor ou o líder da equipe poderá validar todos os trabalhos de entrevistas e pesquisas realizados, conferindo qualquer tipo de inconsistência ou de lacuna de informação.

3.2.2.8. Recomendações

O modelo EDRM apresenta várias recomendações para a fase de identificação. A saber:

- Desenvolver um plano de identificação que possa ser utilizado repetidas vezes. Desta forma, mesmo para casos simples, o plano guiará a equipe por todo o processo, assegurando que todos os pontos importantes serão contemplados.
- Descrever claramente as atribuições e expectativas no plano, definindo os papéis dos membros da equipe e suas respectivas responsabilidades.

- Criar uma lista de sistemas e um mapeamento de dados para fins de elaborar uma lista com os tipos de dados e onde estão armazenadas.
- Incluir no plano as informações relevantes identificadas no processo judicial e no decorrer da investigação.
- Desenvolver um questionário padrão de entrevistas e de pesquisa que poderá ser reutilizado em outros casos.
- Elaborar um portfólio de aplicativos, sistemas, fluxos de dados e serviços das áreas de negócio para fins de identificação de fontes de ESI relevantes.
- Determinar que tipos de arquivos e sistemas podem conter informações relevantes (ex: e-mail, pastas de arquivos, mensagens instantâneas, etc.).
- Determinar uma lista de palavras-chave e tipos de dados para verificar quais as informações que devem ser coletadas.
- Verificar as atualizações a serem implementadas e seus possíveis impactos na consolidação de dados ou migração.
- Levantar todas as fontes e o local de armazenamento de dados (ex: computadores locais, servidores de rede, nuvem, backup, media externa, dispositivos portáteis, *notebooks*, *tablets*, pendrives, computadores particulares, intranet, extranets, etc.).
- Verificar se existem sistemas com deleção de dados automática, limpeza de dados ou que sobrescrevem os dados, de forma a preservar as informações que são relevantes.
- Revisar a Política de Retenção de Dados.
- Documentar processos, ferramentas e metodologias usadas na investigação.
- Providenciar relatórios de acompanhamento e status dos processos de identificação.
- Coletar documentação referente ao processo de identificação como políticas de TI, organogramas, fluxogramas, diagramas que possam impactar no trabalho de *e-Discovery*.
- Registrar toda a documentação utilizada no processo de identificação para fins de comprovação em juízo, como exemplo: a estratégia e o plano de identificação, entrevistas, pesquisas, logs, etc.

- Criar um controle de qualidade e um plano de validação de todo o processo de identificação para verificar sua viabilidade.

3.2.2.9. Riscos

O modelo EDRM apresenta vários riscos que devem ser considerados na fase de identificação, a saber:

- Não desenvolver um plano de identificação, o que pode resultar em processo caótico, não documentado e não viável do ponto de vista legal.
- Não identificar de forma clara as atribuições e as expectativas do plano, o que pode acarretar em resultados inconsistentes, incompletos ou negligenciados.
- Não elaborar uma lista de sistemas ou um mapeamento de dados, o que pode levar ao aumento dos custos do processo de identificação.
- Manter uma lista de sistemas e de mapeamento de dados desatualizados, o que pode resultar em perda de informações.
- Não manter uma lista das áreas e das pessoas que conhecem as informações relevantes da organização, o que pode resultar em perda de informação e dificultar a gestão do conhecimento.
- Não elaborar um questionário padrão de entrevistas e pesquisas, o que pode aumentar o custo de investigação.
- A não inclusão de pessoas apropriadas na equipe de identificação, o que pode representar uma lacuna na identificação de dados relevantes.
- Não identificar de forma devida as fontes relevantes de informações, o que pode resultar em informações incompletas e desnecessárias.
- Não identificar a relevância de determinados tipos de arquivos e sistemas, listas de palavras-chave e tipos de dados, o que pode resultar em maior custo de preservação desnecessária de informação.
- Não levantar o plano de migração, de atualização e consolidação de dados, o que pode levar à perda de informações.
- Não identificar as fontes e o local de armazenamento de dados, o que pode acarretar em perda de informações.
- Não identificar os sistemas de deleção automática, limpeza de dados, ou se os dados são sobrescritos, o que pode resultar em perda de informações.

- Não ter ou não revisar a política de retenção após identificar fontes relevantes de ESI, o que pode resultar em perda de informação ou na ineficiência da política de retenção.
- Não certificar o processo de identificação, o que pode prejudicar a confiabilidade do processo.
- Não providenciar um relatório de acompanhamento e status do processo, o que pode elevar os custos de gerenciamento e o orçamento corrente da investigação.
- Não coletar a documentação relativa ao processo de identificação, o que pode impactar no alcance da investigação. Da mesma forma, em relação à criação e manutenção do plano de identificação.
- Não criar um plano de controle de qualidade e validação, o que pode gerar um processo de identificação ineficiente.

3.2.3. Preservação

Após a fase de identificação, passa-se para a fase de preservação dos dados considerados relevantes para o processo de *e-Discovery*. Esta fase é muito importante tendo em vista que seu objetivo é garantir validade jurídica dos dados coletados ou preservados. Além disso, é importante diminuir os riscos de que evidências encontradas no ESI sejam alteradas ou eliminadas.

Conforme apresentado na Figura 3.5, é importante que os responsáveis pela preservação dos dados estabeleçam uma estratégia de preservação. É importante que seja suspensa a destruição ou eliminação de quaisquer dados armazenados, seja em mídia ou em servidores de rede, que poderão ter relevância no processo de descoberta eletrônica do caso em questão.

A equipe responsável deve elaborar um plano de preparação de preservação que demonstre a fonte dos dados, o local e os tipos de dados que devem ser preservados, bem como a metodologia de seleção e preservação que será utilizada.

Por último, executa-se o plano de preservação conforme descrito no processo apresentado na Figura 3.5. Para cada etapa desse processo deve ser preparado um relatório de progresso e status, mantendo-se toda a documentação necessária para caso de auditoria.

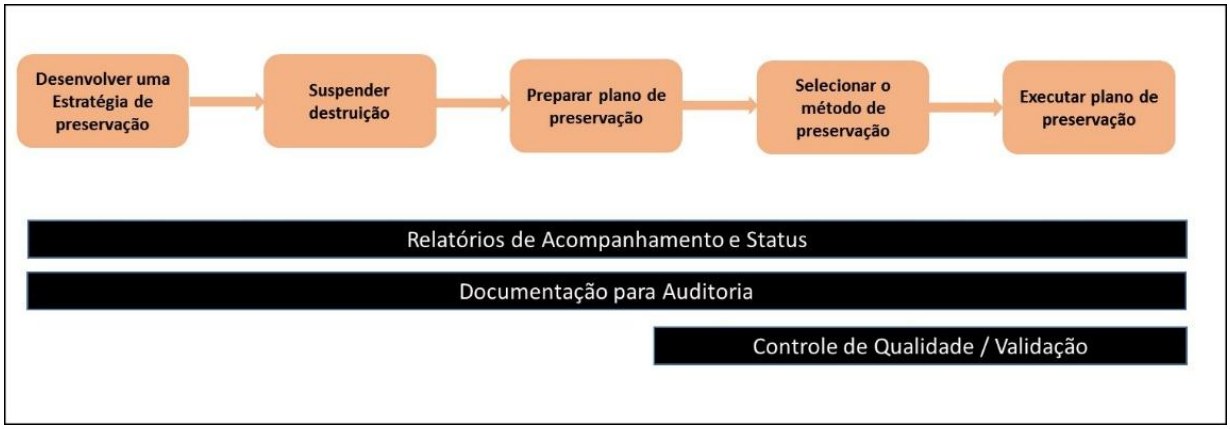

Figura 3.5 - Fluxo para Preservação (EDRM, 2010, tradução).

3.2.4. Coleta

A coleta é a aquisição de informação preservada e identificada como potencialmente relevante na fase de identificação do modelo EDRM. É importante que a coleta de dados seja realizada em conformidade com a legislação, incluindo os metadados associados, de forma a não invalidar o seu valor probatório em juízo. Da mesma forma, o estabelecimento de um processo de coleta contribuirá para eventuais investigações governamentais ou internas.

Cabe destacar que esse processo servirá de retroalimentação para a função de identificação, uma vez que o processo de *e-Discovery* poderá ser ampliado em razão do impacto gerado na fase de coleta de informações eletronicamente armazenadas.

Ao analisar a Figura 3.6, observa-se que o processo de coleta segue a mesma estrutura utilizada no processo de preservação.

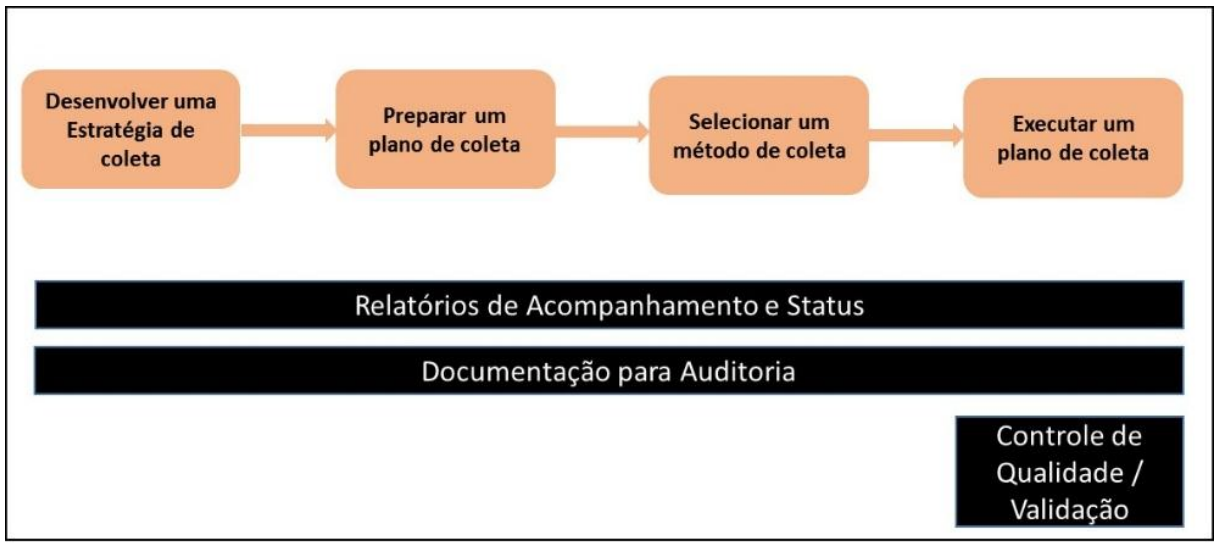

Figura 3.6 - Fluxo para Coleta (EDRM, 2010, tradução)

3.2.5. Processamento

Para que se dê o devido andamento ao ciclo de vida do *e-Discovery*, as fases de identificação, preservação e coleta são necessárias antes de dar prosseguimento para a fase de processamento. Nessa fase é feito um filtro para selecionar as evidências que são mais relevantes para a próxima fase do modelo EDRM: a fase de revisão. A seleção pode seguir critérios diversos, seja com base no conteúdo ou em metadados dos itens selecionados. Tudo deve ocorrer com a estrita aderência ao processo de auditoria, de controle de qualidade, análise e validação e a cadeia de custódia.

Geralmente os dados coletados se apresentam em diferentes formatos e podem estar armazenados em diferentes mídias, demandando em alguns casos a necessidade de restauração. Documentos contidos em arquivos e mensagens eletrônicas podem estar presentes em arquivos compactados (ex: PST, NSF, zip, rar, etc.) e existem aqueles que necessitam ser convertidos para outros formatos a fim de facilitar ainda mais as buscas e filtros da fase de processamento. Durante esta fase esses itens serão catalogados e associados aos metadados capturados.

Raramente é necessário rever minuciosamente todos os itens que são enviados para processamento, sugere-se trabalhar com uma amostra do quantitativo coletado, que poderá ser definido a critério da organização. O processamento é divido em quatro principais etapas: avaliação, preparação, seleção e saída. A etapa de avaliação verifica quais os dados que devem ser mantidos no processo. Preparação envolve atividades de extração, indexação e *hashing*, etc. Seleção envolve a deduplicação de dados; pesquisa e o uso de métodos analíticos para a escolha

dos itens que deverão prosseguir no processo. A saída é a entrega dos dados selecionados em diferentes formatos. As próximas subseções serão as etapas do fluxo de processamento.

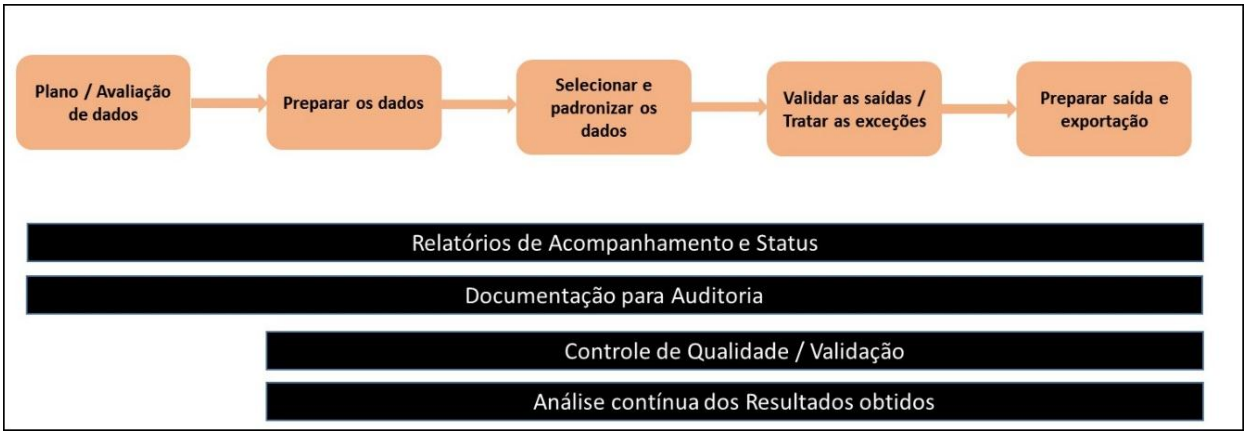

Figura 3.7 -Fluxo para Processamento (EDRM, 2010, tradução)

3.2.5.1. Plano/Avaliação de dados

A avaliação é o primeiro passo da fase de processamento e é considerado crítico, uma vez que permite o correto alinhamento daquilo que será buscado com a estratégia geral adotada do processo de *e-Discovery* do caso em questão. A equipe deve identificar quais otimizações de processamento são necessárias para cumprir com o propósito da investigação. Em outras palavras, esta etapa é importante para garantir que a metodologia de processamento produza os resultados esperados em termos de esforço, tempo, custo, bem como adote estratégias para identificar os dados de saída que sejam relevantes para a investigação.

É imperativo que uma estratégia de controle de qualidade apropriada seja desenvolvida ainda na fase inicial antes de se dar continuidade nas demais atividades do processamento. Isto deve incluir a metodologia, objetivos, expectativas, relatórios e tratamento de exceções. Um elemento crítico de sucesso é o estabelecimento de um plano de comunicação.

Pontos a serem considerados durante a etapa de avaliação:

- Quais dados devem ser processados.
- Quais complexidades/pontos problemáticos geralmente associadas ao processamento desses dados, incluindo informações adicionais, são necessárias ao correto processamento.
- Quais metodologias de processamento tem mais probabilidade de serem bem-sucedidas.

- Quais as estratégias serão utilizadas.
- Quais os fatores de riscos envolvidos (ex: erros de mídia, dados de origem, grande volume de informações, etc.).
- Qual o controle de qualidade a ser adotado.
- Como serão tratadas as exceções.
- Quais as trilhas de relatórios e auditorias serão adotadas.
- Qual o critério de aceitabilidade.
- Quais os formatos de apresentação dos dados de destino e em que mídias ou meios deverão ser entregues.
- Qual o modelo de relatório e plano de comunicação a ser adotado.
- Qual o cronograma de entrega.
- Quais os papéis e responsabilidades definidos.
- Qual o critério de sucesso.

3.2.5.2. Preparar os dados

Durante a etapa de preparação de dados é realizada uma série de atividades a fim de permitir o adequado manuseio e a redução de dados, conforme exposto a seguir:

- Restauração de backups e outros conjuntos de arquivo de dados;
- Conversão de formatos legados e outros tipos de arquivos;
- Extração e descompactação de arquivos;
- Catalogação de todos os arquivos extraídos, e-mails e anexos;
- Deduplicação de arquivos com o uso de *hashing*;
- Identificação entre similaridade entre arquivos por meio de *fuzzy hashing*;
- Identificação e extração de conceito[25];
- Indexação de documentos; e
- Identificação e tratamento de exceções.

[25] Uma tarefa vital para a extração de informação de textos é a identificação de conceito, que nada mais é que o uso de uma ou mais palavras-chave ou definição de texto. Geralmente se utiliza uma ferramenta de mineração de textos para facilitar a identificação de conceitos chaves e relevantes para uma área temática específica. (AKHGAR et al., 2015).

3.2.5.3. Selecionar e padronizar os dados

Uma das principais razões para a execução da fase de processamento em um processo de *e-Discovery* é que se tenha como produto final uma seleção razoável dos dados que seguirão para a fase de revisão pela equipe *e-Discovery*, em particular, advogados. A etapa de seleção e padronização tem como objetivo a redução da quantidade de dados que terão que ser analisados nas fases subsequentes. Após a etapa de preparação há uma série de técnicas para selecionar os itens realmente relevantes e descartar os não-relevantes. O próprio uso de busca por termos específicos pode ser aplicado como parte de uma abordagem válida para identificar itens sujeitos à fase de revisão. Extração de conceito e outras formas de identificação de documentos similares podem ser utilizadas para classificação dos itens para facilitar o trabalho dos profissionais de *e-Discovery* durante a fase de revisão.

3.2.5.4. Saída

Os dados que foram processados e selecionados para a fase de revisão podem ser entregues em diferentes formatos, a depender dos requisitos solicitados inicialmente.

Esta etapa pode ser utilizada para identificar e corrigir eventuais problemas que tenham surgido na fase de processamento. Por isso, aconselha-se a implementação de procedimentos de controle de qualidade para confrontar os resultados alcançados com as expectativas previamente mapeadas, incluindo a identificação das exceções encontradas. Os desvios significativos precisam ser contabilizados por meio de relatórios de auditoria demonstrando os resultados produzidos e as diferenças encontradas. Às vezes os processos *e-Discovery* não alcançam um resultado satisfatório devido a uma série de questões, tais como a falta de informações suficientes quanto ao fluxo de dados, formatação final mal definida ou pela pressa em produzir resultados, podendo gerar retrabalho e aumentar o custo de processamento.

3.2.5.5. Análise Geral / Validação

O modelo EDRM sugere que sejam adotadas práticas de análise e validação com intuito de que problemas ou inconsistências sejam encontradas o quanto antes no processo, evitando assim retrabalho ou falhas. Destacam-se a seguir algumas oportunidades de análise e validação:

- Avaliação: Durante esta etapa, amostras representativas de certos tipos de dados podem ser verificadas para determinar exatamente os tipos de dados desejados e

se são relevantes para o processamento. As amostras realizadas podem orientar quanto à decisão sobre o nível de processamento e de preparação que será necessário para realizar de forma adequada a seleção do subconjunto de dados.

- Preparação: Durante esta etapa do processamento as amostras representativas podem ser analisadas de forma a verificar a eficácia na preparação de diferentes tipos de dados. Não server para determinar se um subprocesso funcionou adequadamente, pois isso seria realizado pelo controle de qualidade, mas sim para verificar se a aplicação do subprocesso é necessária e se agrega valor ao processo geral. Um exemplo é a indexação de texto. Por exemplo, o controle de qualidade pode verificar se o documento em PDF foi devidamente indexado. Já o processo de validação irá verificar se o texto indexado daquele PDF é de fato o conteúdo do documento.
- Seleção: A etapa de seleção pode oferecer oportunidades mais úteis para a fase de Análise, uma vez que uma amostragem dos resultados de termos de pesquisa aplicados nesta etapa pode apontar para a precisão dos conjuntos de itens selecionados. A revisão por amostragem pode alertar a equipe de *e-Discovery* de potenciais falhas na abordagem adotada, principalmente quanto à duplicidade ou à supressão de dados.
- Saída: Verificando as amostras de dados de saída pode-se adicionar um nível de segurança para que o esforço empregado esteja realmente produzindo os resultados desejados. Na medida em que resultados inesperados são encontrados, pode-se adotar as correções necessárias.

3.2.5.6. Controle de Qualidade

O Controle de Qualidade envolve testes para verificar se os processos técnicos foram realizados de forma esperada, independentemente dos resultados encontrados (a análise dos resultados encontrados cabe ao processo de validação).

3.2.5.7. Relatório Geral

Considerando que as tarefas do processo de *e-Discovery* em questão sejam tratadas como parte de um projeto, o líder da equipe pode valer-se de relatórios de acompanhamento e

status como forma de integrar as partes interessadas. É importante que o líder da equipe de *e-Discovery* tenha documentado todas as decisões tomadas durante a fase de processamento.

3.2.6. Revisão

A revisão de documentos é um fator crítico para a maioria dos litígios, uma vez que é usada para identificar documentos sensíveis e relevantes para o caso judicial. É o momento em que a equipe jurídica pode começar a ganhar uma maior compreensão das questões apresentadas em um caso, cujas estratégias jurídicas podem surgir e se desenvolver-se com base no tipo de informação que é encontrada no conjunto de documentos. Haverá inevitavelmente diferentes estratégias para revisão dos documentos. No entanto, os traços comuns dessas estratégias são: entender o alcance da revisão; estabelecer um processo de supervisão e gerenciamento dos revisores; e selecionar os fornecedores, ferramentas e plataformas para revisão adequadas às necessidades da organização.

Durante a fase de identificação, o processo de *e-Discovery* pode minerar um enorme volume de dados. Ocorre que os avanços nas tecnologias de armazenamento de dados, banco de dados, pesquisa e nas funcionalidades dos sistemas de revisão, tem ofertado opções cada vez mais eficientes para lidar com grandes volumes de dados e simplificar o processo de revisão. Além disso, tecnologias emergentes na área de *Big Data* e métodos de pesquisa baseados em conceitos, dentre outras, vem sendo utilizadas com o propósito de fornecer capacidades de pesquisa avançadas. Uma compreensão dessas tecnologias e ferramentas tornou-se uma parte importante da fase de revisão.

Esta fase considera diversos fatores na preparação para a revisão de documentos. Cinco etapas compõem esta fase: desenvolvimento de uma estratégia / plano de revisão, local de revisão / treinamento, fluxograma de análise de dados, condução da revisão e um plano de avaliação e encerramento, conforme apresentado na figura 3.8.

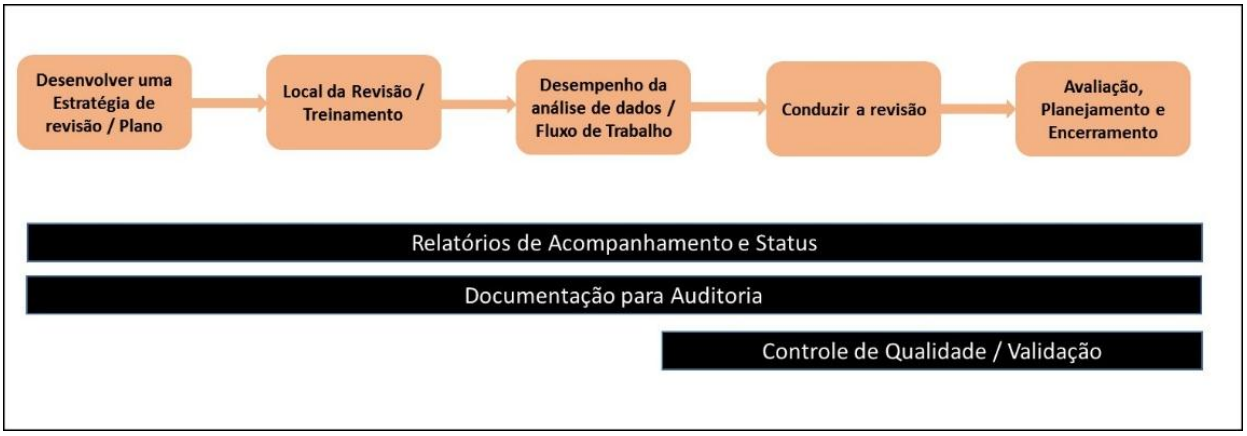

Figura 3.8 -Fluxo para Revisão (EDRM, 2010, tradução)

3.2.6.1. Desenvolver uma estratégia de revisão

São inerentes às atividades do advogado a revisão de todos os documentos que lhes são apresentados, tanto pelo cliente como pela outra parte. Com a popularização do e-mail e outros documentos eletrônicos, acrescido do crescente volume de vestígios tecnológicos produzidos por cada indivíduo, a revisão de todos os documentos eletrônicos, relacionados a um caso pode ser uma tarefa impossível de ser realizada. Uma estratégia-chave é o gerenciamento do trabalho de revisão por meio do uso de tecnologia ou por outros meios que deverão ser discutidos e acordados durante as reuniões iniciais de planejamento desta etapa. Algumas técnicas podem ser úteis para limitar o escopo da revisão, as quais incluem:

- Coleta Estratégica dos dados: pode ser apropriado fazer um segundo nível de seleção (uma coleta mais seletiva dos dados relevantes, em vez de uma revisão em todas as informações selecionadas na fase de coleta) com base em tipos de arquivos ou pastas de arquivos pessoais.
- Filtragem estratégica dos dados coletados – o que pode assumir a forma de aplicação dos limites de data e/ou filtros de palavras-chave nos dados que foram coletados.
- Manter o ESI em seu formato original ao invés de convertê-lo para outros tipos de formatos.

Além de limitar o escopo, é necessário definir se a descoberta deve também englobar documentos em formato físico tradicional, como por exemplo documento em papel.

Uma vez que o escopo seja definido, é essencial a escolha de um gestor de revisão para gerenciar a equipe de revisão. O gestor de revisão deve assegurar que aqueles que foram selecionados para conduzir o processo de revisão estejam alinhados com o método de trabalho

e os objetivos a serem alcançados. Além disso, deverá ser criado um organograma para assegurar que todas as partes envolvidas com a revisão tenham ciência do seu papel. Muitas das vezes, a equipe de revisão contém membros do conselho corporativo da organização, advogados externos e revisores terceirizados.

O gestor de revisão deve criar uma documentação clara das questões-chave e uma distinção entre as questões de fato e as questões de direito.[26] Esta documentação é geralmente elaborada na forma de um manual de orientação para a equipe de revisão. Essas orientações devem identificar o escopo da revisão, o que deve ser procurado e quais os tipos de documentos que podem conter os diversos tipos de evidências relacionadas ao caso. Uma compreensão dos principais atores e dos papéis que cada um desempenhará no caso tende a corroborar com a capacidade da equipe de revisão na identificação e aprimoramento das evidências mais relevantes. Muitas vezes isso ajuda a criar uma rede de relacionamentos entre os atores do caso e as evidências que eles produziram.

Os objetivos de revisão podem evoluir concomitante com a progressão do litígio. Quando isso acontece, é de responsabilidade do gestor da revisão atualizar as diretrizes de revisão para que permaneçam em conformidade com o andamento do caso. Seguem alguns tipos de revisão que podem ser realizadas:

- Determinar a relevância das informações ou documentos colhidos ou produzidos;
- Utilizar campos de banco de dados, marcas ou etiquetas dentro do sistema de revisão para categorizar documentos;
- Determinar a adequabilidade da classificação ou não dos documentos;
- Determinar quais os pedidos de documentos são passíveis de atendimento;
- Identificar os documentos que devem ser marcadas como confidencial ou que tenha apenas alguma parte que pode ser reproduzida;
- Relacionar os principais documentos a supostos fatos ou questões legais anteriormente descritas no caso; e
- Relacionar documentos-chave e os atores do caso que podem depor sobre os respectivos documentos.

[26] Questões de fato estão relacionadas ao problema em si, as condutas e aos fatos concretos. As questões de direito abrangem os aspectos legais, o direito aplicável ao caso, etc.

Em algumas circunstâncias, uma única revisão pode abranger todos estes objetivos. Em outros, a revisão é realizada em etapas, e por diferentes colaboradores.

Todos os membros da equipe de revisão devem estar a par de quaisquer solicitações, bem como de todas as respostas produzidas. A equipe de revisão deve ser treinada no processo e ferramentas utilizadas.

3.2.6.2. Local da Revisão / Treinamento

Dependendo das necessidades do caso, um local específico dentro da organização pode ser definido para o processo de revisão. A equipe de revisão também pode trabalhar remotamente ou dentro de seus escritórios individuais, embora isso possa exigir uma maior necessidade de comunicação interna. Em qualquer caso, o ambiente de revisão deve ser bem iluminado, estar livre de distrações, ruído exterior, e estar devidamente protegido contra entrada de pessoas não autorizadas.

O ambiente de revisão de documentos também deve incluir tecnologias adequadas que permitam a revisão sem interrupções técnicas ou falhas de software, a fim de assegurar o adequado fluxo de trabalho. Caso seja necessário, deve-se designar um técnico para suporte local. Além disso, informações de contato do suporte técnico devem estar disponíveis e divulgadas para toda equipe de revisão.

O recurso tecnológico necessário deve fazer parte do processo de planejamento inicial, a fim de garantir a instalação e o funcionamento adequado do hardware e software de suporte à fase de revisão. Uma vez que a revisão foi iniciada, o suporte técnico deve estar prontamente disponível para resolver quaisquer problemas que possam ocorrer.

A revisão poderá ser realizada on-line, mas mesmo assim o revisor ainda precisará de um espaço de trabalho adequado para espalhar o material de referência e os documentos do caso.

Os revisores tendem a tornar-se cada vez mais familiarizados com o conjunto de documentos a serem analisados e isso propicia a formatação de um padrão na coleta que facilita a determinação quanto à relevância e à importância dos dados. É importante que o conhecimento adquirido por um revisor seja compartilhado de forma rápida e fácil com toda a equipe. Isso poderá ser feito via e-mail, mensagens instantâneas ou em reuniões diárias, de preferência na forma presencial. Dessa forma, os membros da equipe podem livremente discutir e avaliar não só novas ideias, mas também os problemas encontrados.

O treinamento da equipe de revisão, provavelmente, é o componente mais importante para o sucesso da análise de documento eletrônico, pois é fundamental garantir eficiência e precisão, caso contrário, a revisão será provavelmente ineficaz ou mesmo incompleta.

Destaca-se que o líder da equipe deve realizar uma reunião com todos os membros logo no início dos trabalhos para discutir as questões do caso, explicando em detalhes o objetivo da revisão e as informações pertinentes ao caso. Um manual poderá ser usado como uma ferramenta de referência pela equipe durante todo o projeto. Este documento deve ser atualizado durante todo o curso da revisão à medida que surgem novas questões ou novos requisitos.

Algumas das informações discutidas na reunião inicial e presentes no manual podem ser:

- Especificidades do pedido de documento;
- Fatos ou questões da revisão;
- Códigos a serem utilizados para definir os problemas do assunto;
- Privilégio e Confidencialidade; e
- Documentos importantes ou altamente relevantes.

A equipe de revisão também deverá ser orientada no que diz respeito aos documentos altamente relevantes ou "chaves", bem como documentos que requerem especial atenção com base em privilégios ou em confidencialidade.

O treinamento da equipe deve ser específico para as ferramentas que serão utilizadas.

3.2.6.3. Desempenho da análise de dados / Fluxo de Trabalho

As características e funcionalidades fornecidas pela plataforma de revisão servirão para moldar o fluxo de trabalho e é, provavelmente, um dos fatores mais importantes ao escolher o fornecedor do sistema. Para que haja um melhor aproveitamento do trabalho de revisão é importante que a plataforma disponibilize funções como marcar texto, criar seleção de itens favoritos, serviço de busca, leitura de logs, relatórios, etc.

Quanto ao serviço de buscas a ferramenta poderá utilizar a função booleana básica ou outra busca robusta do texto e metadados dos documentos. Frase, proximidade, conceito, e outros tipos de ferramentas de busca são benéficas. Entretanto, o mais importante é a estratégia de revisão. O sistema deve permitir a classificação dos resultados por vários critérios, tais como data, custodiantes, linha de assunto, dentre outros. A velocidade de busca terá impacto sobre

cada operação, e, portanto, o desempenho do sistema deverá ser considerado. O sistema deve também permitir o rastreamento dos resultados dos itens produzidos.

O sistema deve gerir de forma eficaz todo o processo de revisão e apresentar relatórios que subsidiem o trabalho da equipe. Estes relatórios devem ser produzidos diariamente, ou de forma automática, conforme customizado no sistema. Seguem algumas sugestões de relatórios:

- Relatório de Produtividade diária de cada revisor;
- Documentos avaliados diariamente;
- Relatório de rastreamento de dados; e
- Relatórios de Cadeia de Custódia.

3.2.6.4. Conduzir a revisão

A fase de revisão inclui descartar documentos irrelevantes, bem como identificar documentos importantes para a investigação. O que pode determinar a relevância ou não de um documento depende do ponto de vista e da linha adotada pela defesa ou acusação. A definição de critérios de eliminação de documentos irrelevantes poderá necessitar do apoio de uma assessoria jurídica para confirmar, por meio da realização de uma análise mais detalhada dos documentos eletrônicos encontrados, aqueles que de fato não possuam relevância ao caso. Isso poderá envolver também um especialista em suporte a litígios ou provedor de serviços de *e-Discovery* para automatizar a identificação de documentos irrelevantes conhecidos, com objetivo de reduzir a carga de trabalho dos revisores. Muitas ferramentas de detecção eletrônica fornecem métodos automatizados para esse tipo de exclusão. As informações, armazenadas eletronicamente ao serem revisadas, diminuem a necessidade de codificação bibliográfica[27] (ex: data, autor, destinatários, título etc.) pois essas informações são inseridas em campos de banco de dados, o que propicia a busca e recuperação de documentos de forma rápida. Quando os documentos em papel são convertidos em imagens, é necessário o uso de tecnologias adicionais como o OCR, que fornece capacidade de pesquisa de todo o texto.

Após a eliminação de documentos irrelevantes, a equipe de revisão estará pronta para lidar com a tarefa de revisão de documentos que precisam ser selecionados para compor o conjunto de documentos descobertos e farão parte do litígio.

[27] Codificação bibliográfica também é conhecida com codificação legal que é o processo de criação de um sumário ou palavras-chave de um documento. Esse termo é mais utilizado por profissionais da área do direito com a finalidade de criar indexadores para busca rápida ou para construção de um banco de dados para uso em casos judiciais.

Os documentos poderão ser divididos em volume para que cada revisor analise uma faixa específica de artefatos e que não interfira no trabalho de outros colaboradores. Os documentos que apresentam nível de sigilo e privacidade deverão ser revistos antes de serem distribuídos para a revisão.

A equipe de revisão poderá capturar documentos eletrônicos que se relacionam com os principais atores e problemas conhecidos no caso. Os revisores poderão fazer uso de tabelas de consulta a partir de uma lista pré-preenchida de opções de busca, ou também fazer uso de um banco de dados específico que contenha uma série de marcadores que facilitam a categorização da informação. Muitas vezes o resultado de uma busca pode revelar o nome de um envolvido-chave escondido nos metadados de um documento eletrônico. Este é um argumento para a coleta e indexação das informações em formato nativo, evitando perda de informação.

É essencial decidir pela inclusão ou não de documentos em língua estrangeira. Caso sejam incluídos é importante saber se a ferramenta *e-Discovery* dispõe de funcionalidade para trabalhar com outros idiomas. Dependendo do caso, poderá ser necessária a participação de um tradutor juramentado para tradução dos documentos para o idioma oficial do país ou vice-versa.

3.2.6.5. Avaliação, Planejamento e Encerramento

Nesta etapa da fase de revisão são realizadas avaliações e verificações do que foi planejado foi de fato executado, bem como se os objetivos foram alcançados em termos de prazos, custos e resultados.

3.2.6.6. Relatórios de Acompanhamento e Status

O responsável da equipe de revisão pode valer-se de relatórios de acompanhamento e status como elemento para acompanhamento das atividades executadas. Os relatórios de acompanhamento e status devem responder as seguintes questões:

- Controle de qualidade - Estão todos os documentos no sistema? Os arquivos que apresentaram erro foram tratados? A quantidade de documentos a serem revisados é igual à quantidade de documentos disponíveis?
- Escopo - Discriminação por quantidade e por tipo de arquivo; número de documentos reproduzidos; número de custodiantes; número de documentos irrelevantes, quantidade de documentos que faltam ser revisados.

- Eficiência dos revisores e projeção de custos - Taxa de revisão por revisor por dia / semana / mês e fator de qualidade da avaliação.
- Cumprimento do prazo previsto de conclusão.

A documentação pode incluir relatórios de auditoria, logs e de desempenho de revisores.

3.2.6.7. Controle de Qualidade / Avaliação

Medidas de controle de qualidade devem ser implementadas em cada etapa do processo, de modo que a revisão seja consistente, precisa e defensável. Medidas de controle de qualidade podem evitar a duplicação desnecessária de revisão e ajudar no cumprimento de prazos.

A plataforma de revisão deve permitir que os revisores sinalizem um documento para revisão adicional quando não tiverem certeza sobre como tratá-los. Isso garante que os revisores não terão que tomar uma decisão sobre um documento que ainda está pendente de revisão. Os revisores também devem ser capazes de rever facilmente um documento e alterar a sua classificação sempre que necessário.

A plataforma de revisão também deve ser personalizável o suficiente para permitir que ações de controle de qualidade sejam aplicadas aos conjuntos de documentos, tais como e-mails e anexos.

O monitoramento de controle de qualidade pode incluir uma revisão de segundo nível sobre o total ou sobre uma amostragem tecnicamente válida dos documentos revisados. A avaliação de segundo nível é realizada por outros revisores ou advogados experientes que estejam também familiarizados com a matéria em análise. Isso normalmente é feito no que diz respeito aos documentos classificados com status de privilégio ou protegido.

Além disso, ao invés de uma revisão de segundo nível, o advogado líder da equipe pode realizar o controle de qualidade utilizando outros critérios de forma a verificar se há alguma incoerência no protocolo de revisão. Ambos os casos podem refletir padrões de classificação inconsistentes que, em seguida, podem ser tratados por toda a equipe de revisão. Se possível, sugere-se que isso ocorra diariamente, a fim de identificar os problemas com o processo de revisão ou especificamente com um revisor individual da equipe.

3.2.7. Análise

Embora a fase de Análise, no modelo EDRM, seja subsequente à fase de revisão, ela pode interagir com as demais fases do EDRM, até mesmo em uma fase de pré-descoberta. Por

esta razão, o diagrama apresentado na Figura 3.9 revela todas as fases do quadro EDRM sob o componente de Análise.

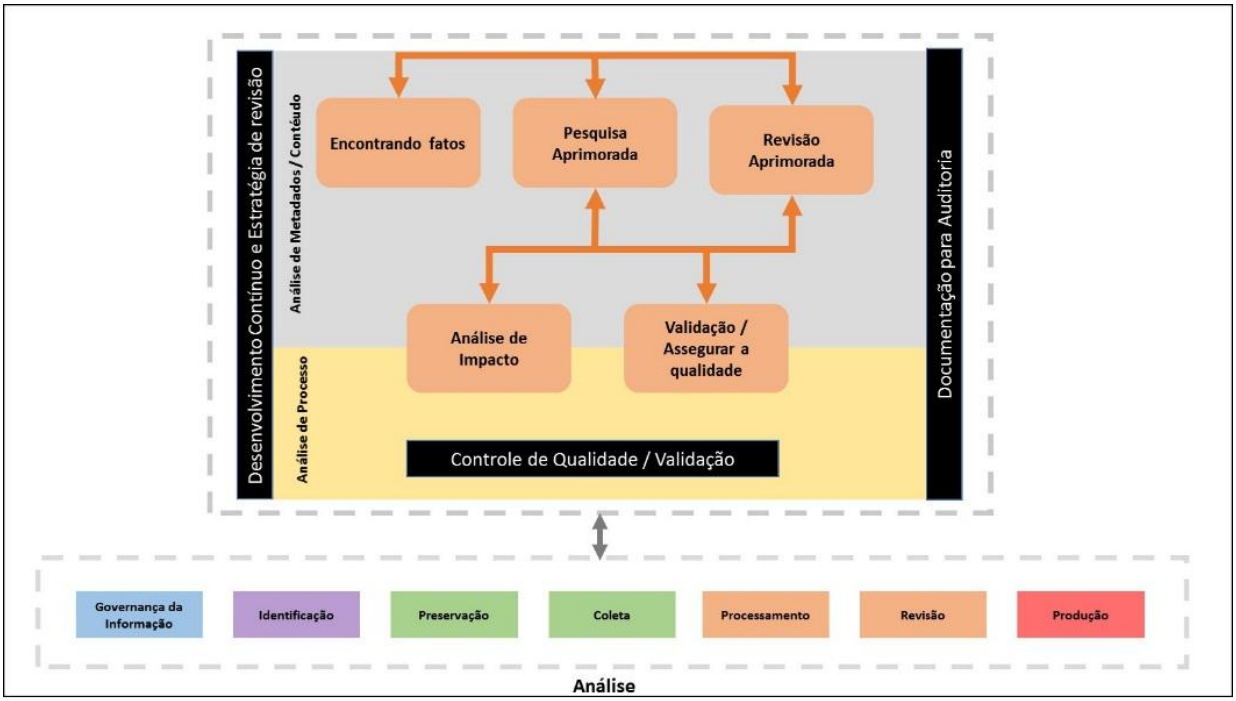

Figura 3.9 - Fluxo da Análise (EDRM, 2010, tradução)

Assim como as ferramentas e processos de *e-Discovery* têm-se aprimorados, métodos sofisticados de análise foram apresentados como forma de ajuda às demais fases da descoberta eletrônica, representados no âmbito EDRM. Quando o modelo foi originalmente concebido, o foco era a análise dos documentos coletados para tornar mais fácil a seleção de documentos e proporcionar uma maior produtividade durante a fase de revisão. Mais recentemente, todos os tipos de análises (descritos a seguir) estão sendo usados para aumentar a produtividade ao longo do processo.

3.2.7.1. Análise de Conteúdo

As três primeiras áreas na análise do diagrama (Figura 3.9) estão agrupadas em análise de conteúdo, com o objetivo de compreender as circunstâncias, os fatos e as evidências potencialmente relevantes em um litígio ou investigação. Por conseguinte, há espaço para atuação da análise de processo e garantia de qualidade dentro das primeiras três seções.

Encontrando os fatos

- Gestão da informação

As organizações têm se atentado em adquirir novos e melhores sistemas de Gestão da Informação (gerenciamento de registros, gerenciamento de conteúdo corporativo e/ou arquivamento). Essas organizações estão em busca de tecnologias de análise de conteúdo para apoio às atividades de infraestrutura. Uma das questões que as organizações estão tendo de lidar é em como reduzir a quantidade de informação armazenada utilizando a Gestão da Informação e os novos Sistemas de Arquivamento. Também estão tendo de lidar com a categorização da sua documentação eletrônica, bem como determinar se um item (arquivo, documento ou e-mail) é um registro relevante para o negócio e se deve realmente ser armazenado.

Geralmente, a sistematização da Gestão da Informação tem sido trabalhada de forma apartada do projeto de *e-Discovery*. A sua inclusão no modelo original de EDRM e o devido tratamento na fase de Análise é uma demonstração de que as organizações devem trabalhar com a Gestão da Informação e com o *e-Discovery* de forma conjunta.

Cada vez mais, os desenvolvedores de sistemas de Gerenciamento de Informações precisam entender não só as nuanças quanto ao uso de informação e do negócio da organização, assim como do gerenciamento de litígios e questões de descoberta eletrônica.

A mudança para soluções de hospedagem de documentos e e-mails em "nuvem" não justifica descartar um projeto de Gerenciamento de Informações. Ambientes que são movidos para nuvem também apresentam o seu próprio conjunto de problemas e devem ser abordadas as razões que justificaram essa decisão, bem como a confiabilidade do prestador de serviços escolhido.

As organizações estão atentas quanto à utilização da análise de conteúdo como sendo um filtro catalogador de informações para fins de descarte, inclusão ou exclusão nos Sistemas de Arquivos. As informações identificadas como não sendo um registro de negócio podem ser mantidas fora do fluxo de *e-Discovery*, o que torna o processo mais eficaz.

Após a crise da Sarbanes Oxley e os incidentes de destruição de documentos amplamente divulgados na mídia, as organizações estão desenvolvendo e implementando políticas de retenção de documentos. Os sistemas de Gestão de Informação devem ser projetados para aderir estritamente à legislação em vigor, que muitas vezes se tornam o foco de exame detalhado durante o processo de *e-Discovery*.

- Preparação para Litígios

Um dos objetivos da Gestão da Informação é estruturar a TI para que informações sejam recuperáveis em casos de litígio. A implementação de um programa de Gestão de Informação robusta contribui para a eficiência, eficácia e economia de custos do *e-Discovery*, contribuindo assim para melhores resultados em eventuais litígios.

As etapas de análise envolvidas na preparação para litígios se sobrepõem às realizadas durante o projeto de Sistema de Gestão da Informação, mas também espelham algumas das tarefas que serão executadas mais tarde no processo *e-Discovery*. Os preparativos de um contencioso não se aplicam a um único assunto, incidente, produto, etc., mas para todos e quaisquer assuntos hipotéticos.

Organizações podem identificar em seu histórico de litígios quais informações são mais relevantes e, antecipadamente, preparar o Sistema de Gestão da Informação para reter os dados com maior chance de serem requisitados. A análise pode contemplar ainda quais as divisões da organização estão mais propensas a ter litígio e, dessa forma, prepará-las antecipadamente.

As políticas e processos de retenção são fáceis de implementar, casos sejam concebidos como parte da infraestrutura geral do Sistema de Gestão da Informação.

- Avaliação de Dados

Uma vez que o litígio tenha sido iniciado, muitas tarefas podem ser facilmente desempenhadas quando uma organização está proativamente preparada para responder a litígios. Com ou sem essa preparação, a equipe de *e-Discovery* se beneficia quando, logo de início, realiza um esforço concentrado para avaliar as informações pertinentes ao litígio ou investigação. O objetivo essencial da avaliação é determinar o trabalho que será desempenhado, as ações necessárias e o impacto de cada decisão.

A avaliação de dados buscará prever a quantidade de dados que deverão ser preservados, coletados e processados; qual a estimativa do custo total do trabalho de *e-Discovery*, possíveis benefícios e riscos dos vários cenários de descoberta. Se o esforço de avaliação for eficaz, a equipe e *e-Discovery* será capaz de estimar um valor relativo dos custos do processo.

Pesquisa Aprimorada

A equipe de pesquisa aprimorada deverá ser capaz de disponibilizar uma grande quantidade de informações sobre o caso, tais como: memorandos, entrevistas, fatos, listas de termos de pesquisas, listas de custodiantes, biografias consultadas, listas de caracteres

elencadas, cronologia do caso, pronunciamentos e respostas aos interrogatórios. Para que haja credibilidade em juízo, a equipe de pesquisa aprimorada precisa apresentar os métodos e critérios utilizados na redução do universo de informações processadas sobre o caso, justificando assim a relevância das informações apresentadas.

Revisão Aprimorada

As revisões devem aplicar técnicas de "mineração de dados" para fazer agrupamentos automáticos de dados segundo seu grau de semelhança, análise e inferências. Outras ferramentas também podem ser usadas para agrupar documentos, que possam colaborar ou acelerar a revisão. Os litigantes devem estar sujeitos a seus próprios procedimentos de controle de qualidade.

Um dos passos mais importante da elaboração de análises é garantir que as ferramentas de revisão possam rastrear os resultados dos trabalhos dos revisores para cada documento analisado.

O foco principal da revisão aprimorada é a realização de verificações lógicas para averiguar se os resultados alcançados estão dentro da expectativa do esperado.

3.2.7.2. Análise de Processo

As duas últimas áreas da Figura 3.9 estão agrupadas na Análise de Processos e se atém a compreender a eficácia dos métodos utilizados durante o *e-Discovery* e as decisões tomadas com base na análise.

Análise de Impacto

A etapa de Análise de Impacto é necessária para comparar o impacto de um sistema novo ou modificado na Gestão da Informação. Implica em verificar as ameaças quanto à análise do litígio. Os analistas devem rever os resultados dos litígios utilizando-se de auditoria ou preservação dos dados coletados. O Relatório de Análise de Impacto deve se direcionar a verificar os seguintes detalhes:

- O cumprimento das políticas de retenção de documentos;
- A quantidade de dados que deveriam ter sido destruídos, mas que não foram, por isso foram considerados na análise;
- Os dados que deveriam ter sido mantidos e não foram;

- Percentagem de usuários que não estão em conformidade com a Política de Retenção; e
- Percentagem de áreas que não estão em conformidade com a Política de Retenção.

Análise Geral / Validação

As decisões tomadas com base na análise devem ser averiguadas em termos de qualidade, de forma a assegurar e validar os métodos empregados. Um aspecto igualmente importante é que a garantia de qualidade e de validação deve ser realizada em tempo real para que realmente gere resultados significativos para o processo.

Em razão de inconsistências ou falhas que possam ser encontradas no processo, é temerário que sejam tomadas decisões importantes baseadas em informações ainda não verificadas, ou mesmo testadas. É uma boa prática fazer a mesma pergunta em diferentes momentos, de formas diferentes, com pessoas diferentes, especialmente durante o mapeamento de dados e entrevistas de custódia. Da mesma forma, isso se aplica em testar em sistemas diferentes, verificando se os mesmos resultados são alcançados em diferentes sistemas de *e-Discovery.*

A documentação de todo o processo, de preferência, deve ser preservada na medida em que estão sendo executadas as atividades do processo de *e-Discovery*, o que torna o processo mais eficaz e confiável. Os processos de *e-Discovery* que apresentam problemas, geralmente possuem falhas de documentação. Quando um processo é difícil de documentar, o modelo provavelmente terá que ser redesenhado mais cedo ou mais tarde. A documentação deve ser feita em tempo real e incluir todo o planejamento, bem como os resultados alcançados.

3.2.8. Produção

O aumento sem precedentes da quantidade de informações armazenadas eletronicamente (ESI), principalmente no meio empresarial, também gera um aumento correspondente nos dados que deverão ser coletados e revisados, e também na produção para atendimento aos processos judiciais e para as investigações regulatórias. Por causa da complexidade, os custos elevados e os riscos significativos associados à produção de ESI, o tema tem sido abordado nos Estados Unidos em um número crescente de artigos, apresentações

e opiniões jurídicas.[28] Como medida da importância do tema, a produção de ESI está presente diretamente no Código de Processo Civil Federal americano. Por exemplo, a Regra 26 (f) define que o método e formato do ESI devem ser produzidos conforme negociação entre as partes no início do processo de *e-Discovery*. A produção de ESI continua a apresentar desafios no processo de descoberta eletrônica, apesar de as regras específicas nos Estados Unidos terem sido elaboradas e aprovadas para resolução de problemas.

O diagrama apresentado na Figura 3.10 revela todas as fases do quadro EDRM sob o componente de Produção.

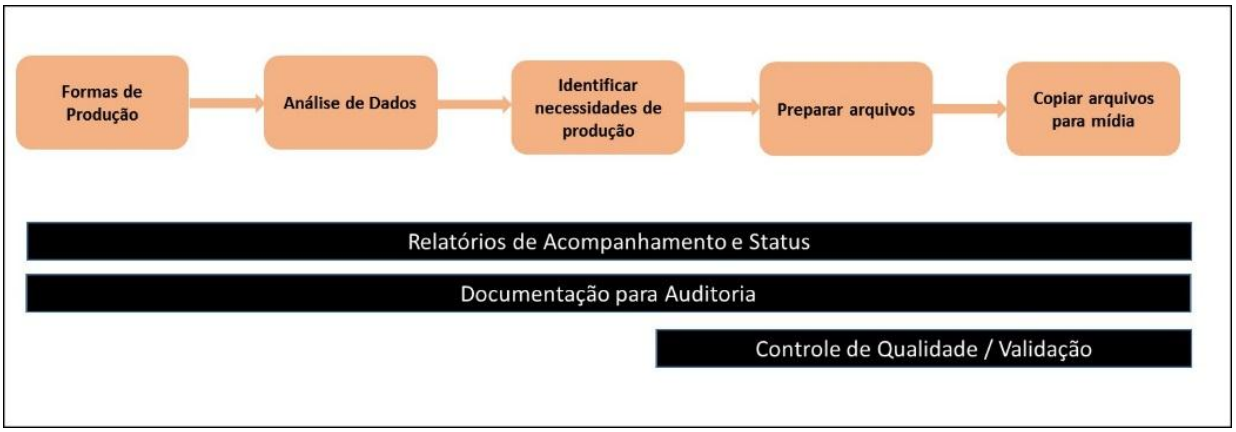

Figura 3.10 – Produção (EDRM, 2010, tradução)

3.2.8.1. Formas de Produção

Antes do *e-Discovery*, a descoberta de evidências era tratada quase inteiramente pela equipe da área de direito. Já na era do *e-Discovery*, o envolvimento da equipe de tecnologia é primordial para garantir uma produção de informações altamente relevantes. A equipe técnica deve ter envolvimento do pessoal de TI da corporação, sejam de cargos efetivos ou até mesmo de prestadores de serviços.

Os membros da equipe técnica podem verificar sobre as formas de produção de ESI antes mesmo do encontro inicial entre as partes, para que seja definido como serão estabelecidos os processos e a análise de dados para garantir a produção eficiente e completa dos documentos recebidos.

[28] Uma busca no google acadêmico de 2000 a 2009 foram encontrados 3.060 registros sobre e-Discovery. Nos últimos 6 (seis) anos, no período de 2010 a 2016, a busca indicou 7.630 registros.

É importante que seja de conhecimento de todos sobre as cópias dos pedidos de documentos que serão solicitadas a outra parte, o método de trabalho que será utilizado, o conteúdo das produções, etc. Estas informações facilitarão a comunicação entre as equipes técnicas e legais sobre o conteúdo e a completude da produção sob o ponto de vista técnico.

A regra 34 (b) do Código de Processo Civil Federal dos Estados Unidos prevê que a parte requerente especifique a forma ou as formas de produção. Se o pedido não for atendido conforme solicitado, a parte demandada deve indicar em sua reposta ao requerente a sua forma ou formas de produção de informações. Para esse caso é importante entender os tipos de ESI disponíveis para a produção, a natureza desse ESI e como vão impactar na capacidade de encontrar as evidências necessárias para produção de informação. Pode ocorrer que a litigante ao receber uma produção de imagens da outra parte não consiga analisar as informações no formato enviado. A justiça pode determinar que seja entregue a documentação em formato nativo, o que irá gerar retrabalho e uma nova produção de documentos. Por isso, entende-se que nas reuniões de tratativas entre as partes, que são realizadas logo no início do processo, os representantes legais das empresas tenham conhecimento desse assunto e que consigam definir de forma clara todos os aspectos de produção de ESI, para fins de coleta, processamento e produção de documentos.

Seguem algumas formas de produção:

- Nativas - Os arquivos são produzidos no seu formato nativo. Esta forma de produção pode incluir arquivos, metadados extraídos e textos pesquisáveis.
- Quase nativas - Os arquivos são extraídos ou convertidos em outro formato pesquisável que se aproxima do formato nativo. Esta produção pode incluir arquivos, metadados extraídos e textos pesquisáveis.
- Imagem (Quase Papel) - Os arquivos são convertidos para arquivos de imagem, normalmente “.tif” ou “.pdf”. Esta produção pode incluir arquivos, metadados extraídos e textos pesquisáveis.
- Papel - ESI é produzido em formato de papel.

3.2.8.2. Análise de Dados

Uma das primeiras etapas da fase de produção é analisar os dados e determinar as formas de produção de informação. Para isso é fundamental entender como os diferentes tipos de documentos afetam a forma (s) de processamento e produção. Por exemplo, as fórmulas não

são visíveis quando planilhas são convertidas em imagem; cópias ocultas e a data de leitura não ficam disponíveis quando e-mails são convertidos em imagem; e notas do apresentador podem não ficar visíveis nas apresentações do MS-PowerPoint, quando essas apresentações são convertidas em imagem. A necessidade de uma determinada informação deve ser feita logo no início do processo de *e-Discovery*. Considerando antecipadamente quais as opções de formas de produção estão disponíveis para determinar qual será utilizada para cada tipo de arquivo, fato essencial no momento de negociação entre as partes quanto às opções de produção, como também para garantia de que a equipe jurídica estará recebendo as informações necessárias e conforme solicitado inicialmente.

3.2.8.3. Identificar necessidades de produção

A produção se refere aos arquivos de processamento de texto, planilhas, e-mail, bancos de dados, desenhos, fotografias, dados de aplicações proprietárias, dados de sites, correio de voz, entre outros. Para saber quais as informações que devem ser produzidas para um determinado caso, é necessário conhecer quais dessas informações estão disponíveis nos diferentes tipos de sistemas existentes na organização. Para produzir os diversos tipos de dados é necessário entender as questões específicas do processo judicial e verificar quais informações estão disponíveis nos diferentes sistemas de software (ou tipos de documentos). Tal preparação atenua o risco de descobrir tarde demais que a forma de produção acordada é insuficiente para proporcionar os elementos necessários para abordar e compreender as questões na disputa ou investigação. Anteriormente o papel era o único formato existente para produção de informação. Atualmente, as produções ESI muitas vezes têm mais do que um componente.

3.2.8.4. Preparação de arquivos

Uma vez que os documentos foram revistos e o conjunto de produção tenha sido determinado, os documentos devem ser preparados para a produção.

A entrega da produção deve ser preparada conforme o protocolo que as partes acordaram durante a audiência inicial, bem como outras diretrizes determinadas durante o processo judicial. Os profissionais de tecnologia devem preparar o conjunto de produção e descrever cada componente produzido. Isto pode ser uma tarefa demandante, uma vez que são necessários vários formatos para os componentes produzidos de forma a atender os requisitos das diversas ferramentas de revisão. A parte receptora pode não estar familiarizada com um formato de

arquivo de extensão específica, pois pode estar usando uma versão diferente do software ou uma ferramenta de revisão completamente diferente. Nestas situações, os profissionais de TI devem comunicar-se diretamente para evitar confusão, frustração, atrasos e custos desnecessários.

Alguns exemplos de preparação de arquivos são:

Formatos de arquivo

Os arquivos de produção são geralmente identificados durante a fase de revisão e exportados a partir do sistema de revisão de documentos.

Em muitos casos, as produções podem conter mais do que um formato de arquivo. Por exemplo, os documentos do MS Word podem ser convertidos em formato de imagem (quase-papel), os e-mails produzidos em formato HTML (quase nativo) e as planilhas MS Excel produzidos em formato nativo. Em outros casos, tudo o que pode ser produzido em formatos nativos ou quase-nativos, exceto quando outros acordos foram estabelecidos entre as partes.

Os arquivos de texto pesquisáveis

Os arquivos de texto pesquisáveis podem ser incluídos na produção nativa, quase nativo e de imagem (quase papel). Para produções nativas e quase nativas, os arquivos de texto pesquisáveis são geralmente convertidos em outro arquivo "txt", sendo o arquivo original e o arquivo "txt" inclusos na produção. Por exemplo:

ABC00001.doc é um documento nativo do MS Word e
ABC00001.txt é um texto de pesquisa.

ABC00002.htm é um arquivo quase nativo de e-mail e
ABC00002.txt é um texto de pesquisa.

Campo de Dados

É importante que os advogados das partes entrem em acordo em relação à lista de campos que serão ou não serão produzidos. Os dados que foram extraídos de documentos eletrônicos são comumente produzidos como campo de dados. Os dados encontrados podem ser produzidos em um arquivo de texto com os nomes de campo na linha de cabeçalho ou em formato XML. Em um arquivo de texto, cada elemento de dados tem um campo de separação e um qualificador de texto. Estes são conhecidos como delimitadores. Por exemplo:

| DocID | Autor | Destinatário | Assunto |
| ABC00001 | Doe,John | Smith,Sue| Orçamento e Financeiro 2016|
| ABC00002 | Doe,John | Jones,Fred| Agenda da Reunião Gerencial|

3.2.8.5. Copiar arquivos para mídia

Os dados podem ser armazenados e entregues em uma grande variedade de meios, que podem incluir CDs, DVDs, discos rígidos (externos) portáteis, pen drives ou um repositório web online. A escolha dos meios de comunicação pode ter impacto significativo na quantidade de tempo e nos custos da disponibilização. O meio é selecionado com base no tamanho da produção. Além disso, devem-se considerar recursos de proteção a escrita e a criptografia da mídia a ser utilizada. Se uma grande quantidade de dados será produzida, pode ser melhor armazená-los em um disco rígido, em vez de dezenas ou centenas de discos ópticos.

A entrega da produção pode ser feita de forma on-line. As entregas on-line envolvem o acesso aos dados de produção pela parte receptora através de um *login* seguro para acesso a um banco de dados via web que pode ser hospedado por um provedor de serviço terceirizado.

3.2.9. Apresentação

A apresentação de informações armazenadas eletronicamente pode ser um desafio para os advogados que atuam no campo de *e-Discovery*. Nas exposições anteriormente realizadas em juízo, as descobertas eram apresentadas em suporte de papel. O desenvolvimento tecnológico ao longo da última década tornou mais fácil a apresentação de exposições em formato digital. A Figura 3.11 apresenta orientações do modelo EDRM para apresentação de informações armazenadas eletronicamente em depoimentos, arbitragens ou julgamentos.

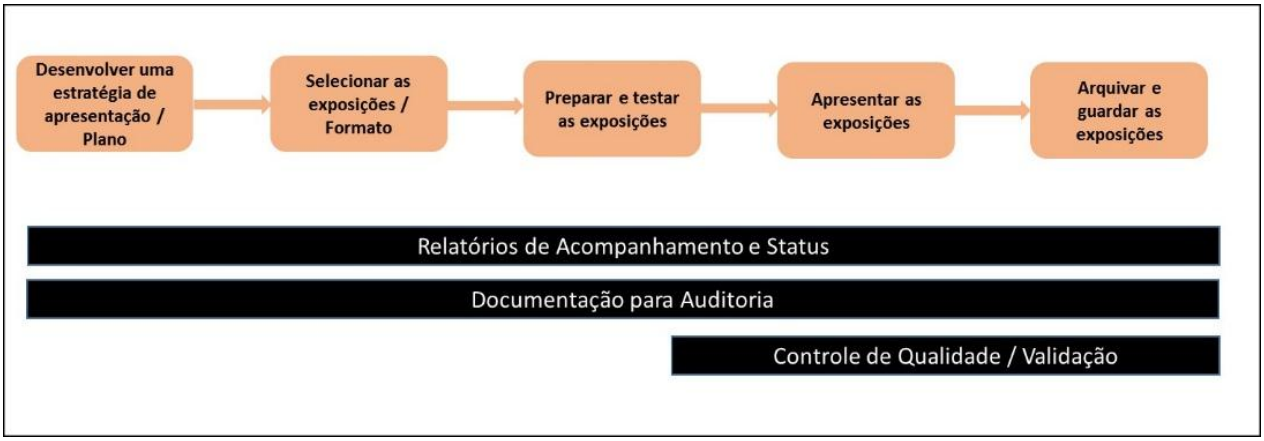

Figura 3.11 - Fluxo da Apresentação (EDRM, 2010, tradução)

3.2.9.1. Desenvolver Estratégia

Metas e Objetivos

A primeira etapa da fase de apresentação é o desenvolvimento de uma estratégia, que deve considerar alguns objetivos e metas, como por exemplo:

- O trabalho de *e-Discovery* realizado busca persuadir ou informar?
- Que histórias ou temas serão comunicados?
- Que fatos serão demonstrados?
- Que outra evidência adicional?
- É necessário estabelecer credibilidade?
- É necessário fornecer contexto e educação para aumentar a compreensão?
- Que tipos de ESI fazem parte do conjunto de produção?
- Os elementos de ESI atingem as metas e objetivos?
- É necessário descrever os procedimentos adotados durante a preparação ou processamento?

Análise jurídica

As provas admissíveis em um tribunal podem ser testemunhais, documentais ou materiais. Para que a prova seja admissível, a evidência deve ser relevante, sem mácula, e deve ter indícios de credibilidade.

Para que a evidência seja relevante, ela deve tender a provar ou refutar algum fato que está em disputa no processo. Se a evidência é na forma testemunhal, a parte deve estabelecer as bases para a credibilidade da testemunha. Boato geralmente é rejeitado por sua falta de

credibilidade. Se a evidência é documental, a parte que apresenta a evidência deve ser capaz de mostrar que a documentação é autêntica e possui lastro na cadeia de custódia.

3.2.9.2. Preparação das Exposições

As exposições em juízo poderão ser feitas de diversas formas, por exemplo:

- Digitalização da documentação;
- Documentos em formato PDF;
- Áudio;
- Vídeo;
- Imagens;
- Softwares de Apresentação (*Powerpoint, Keynote*);
- Gráfico de dados e tabelas;
- Fontes da Internet;
- Banco de Dados, etc.

3.2.9.3. Testes para apresentação

O apresentador deve ter domínio sobre o assunto, bem como a capacidade de comunicar sobre questões técnicas de forma clara e sucinta para um público leigo. Como testemunha, o apresentador deve estar preparado para responder os questionamentos da parte opositora do processo, atuando de forma objetiva e resolutiva. O papel do apresentador é sem dúvida desafiador e gratificante.

Em alguns casos se faz necessária a participação de pessoas altamente especializadas sobre o assunto, mas muitas vezes o trabalho será bem-sucedido se houver o engajamento de toda equipe desde o início do caso.

É importante que a equipe se certifique da condição dos equipamentos que serão utilizados antes da apresentação em juízo. É também fundamental que seja realizado o backup dos dados, bem como um plano alternativo de apresentação, caso ocorra algum fato inesperado. Não se pode dar a chance de perder todo o trabalho que foi realizado e ainda perder o caso na Justiça por não se ter alternativas de apresentação.

3.2.9.4. Apresentação

O dia da apresentação é o dia em que o resultado de todo o trabalho será apresentado em juízo. Tendo em vista todo o preparativo até este ponto do processo de e-Discovery, pode-se dizer que é a coroação do trabalho realizado. Se os resultados alcançados não forem apresentados adequadamente, por melhor que tenha sido o empenho da equipe, o resultado pode ser interpretado de forma insatisfatória pelo júri ou juiz.

3.2.9.5. Armazenamento

A corporação deve desenvolver diretrizes para arquivar e manter a acessibilidade dos materiais dos casos pós-veredicto. Se o caso for objeto de recurso, o material deve ficar acessível e não ser enviado para arquivamento. É possível valer-se do armazenamento em nuvem para disponibilizar o material produzido a diferentes partes interessadas.

3.3. CONSIDERAÇÕES

Este capítulo apresentou um método para análise de caso judicial (FIRAC) e um modelo específico para tratamento do processo de *e-Discovery* (EDRM). O modelo EDRM pode ser considerado um processo iterativo para implementação do *e-Discovery*, muito útil para qualquer organização que busque normatizar ou padronizar seus processos de *e-Discovery*. Serve ainda como um guia para um processo de identificação de dados e sua subsequentemente preservação para a coleta e processamento.

Este capítulo descreveu detalhadamente as diversas etapas do EDRM, conforme o modelo publicado e gerenciado pela *Duke Law Center for Judicial Studies*, da Universidade de Duke em Durham, NC, Estados Unidos da América (Duke Law, 2016). Os conceitos relacionados ao *e-Discovery* e ao EDRM apresentados neste capítulo foram extraídos do glossário do EDRM. (EDRM, 2016).

A descrição do modelo EDRM fez-se necessária para subsidiar as discussões do próximo capítulo, fruto da contribuição principal deste trabalho, em que é explorado como as fases do EDRM podem ser relacionadas aos controles de segurança da informação das normas ABNT NBR ISO/IEC 27001:2013 e 27002:2013. O capítulo 4, portanto, discorre sobre a proposta da pesquisa, apresentando a relação do modelo EDRM e os controles de segurança da informação.

4. PROPOSTA DO TRABALHO

O trabalho propõe a utilização do modelo de Referência de Descoberta Eletrônica, ou, *Eletronic Discovery Reference Model* (EDRM) para o processo de e-*Discovery*, como ferramenta preliminar de identificação e priorização de possíveis melhorias no Sistema de Gestão de Segurança da Informação.

Como apresentado no capítulo anterior, o processo de *e-Discovery* existe para ajudar as organizações a filtrarem, dentre o enorme volume de dados processados e armazenados, aqueles que podem ser relevantes e eventualmente utilizados em procedimentos legais ou disputas judiciais. Como exemplo, cita-se o caso de falência da empresa Enron Corporate, no ano de 2011, considerada então uma das maiores empresas de energia do mundo, a qual envolveu a análise de uma grande quantidade de documentos digitais, em particular e-mails. Segundo Phillips et al (2013), mais de 300.000 e-mails foram utilizados no tribunal como evidências no caso em questão.

Ao tratar grandes volumes de dados relacionados a um dado litígio, as organizações podem encontrar um número considerável de achados/evidências que podem ser decorrentes de falhas de segurança da informação, muitas vezes resultado de uma política de segurança da informação mal elaborada. O controle de acesso à rede de dados, às informações sigilosas, ao serviço de internet e de e-mail podem ser realizados de forma precária, sem uma visão holística do Sistema da Gestão de Segurança da Informação e da Governança de TI, o que pode expor a organização em eventuais disputas judiciais. Devido ao crescente volume de dados, acrescido da heterogeneidade e atualização constante dos sistemas, falhas relacionadas à segurança da informação podem expor legalmente uma organização. Caso a organização não esteja preparada para tratar a descoberta eletrônica de documentos, é possível que, além de responder em juízo às consequências decorrentes de falhas no Sistema da Gestão de Segurança da Informação, a organização pode não ser capaz de prontamente identificar, preservar, coletar e processar as evidências que poderiam servir como prova para defesa ou acusação.

A proposta apresentada permite que uma organização analise como os controles do Sistema de Gestão de Segurança da Informação – SGSI se relacionam com o EDRM, apontando para aqueles que podem ter um maior impacto em eventuais litígios. O que se propõe é que as organizações possam avaliar preventivamente as fases do diagrama do EDRM com o objetivo de verificar a existência de determinados controles de segurança da informação. Desta forma será possível avaliar a necessidade de sua implementação ou, caso já implementados, verificar

a necessidade de seu aprimoramento, objetivando a minimização dos riscos associados a eventuais litígios. Ou seja, a organização pode utilizar o modelo proposto como ferramenta preliminar de identificação e priorização de implementação ou melhorias nos controles do SGSI.

Desta forma, foi realizada uma análise detalhada das fases e etapas do EDRM e sua relação com os controles do Sistema de Gestão de Segurança da Informação – SGSI, conforme descrito nas Normas ABNT NBR ISO/IEC 27001:2013 e 27002:2013. A Tabela 4.2 resume o resultado de alto nível desta interseção de informações e seus impactos, possibilitando a visualização macro de quais controles de segurança são mais relevantes no método de aplicação do processo de *e-Discovery*.

A seção 4.1 apresenta a relação entre o modelo EDRM e o SGSI, seguido da seção 4.2 que apresenta as contribuições do *e-Discovery* para a segurança da informação.

4.1. RELAÇÃO ENTRE O EDRM E O SGSI

Esta seção apresenta como a disciplina Segurança da Informação, uma das práticas de governança de TI, pode se valer do processo de *e-Discovery* para priorização da implantação de controles. De forma simplificada, pode-se entender que os dados identificados como críticos no processo de *e-Discovery* poderão apontar para a necessidade de uma ação de proteção com vistas a assegurar sua disponibilidade, integridade, confidencialidade e autenticidade. A principal vantagem do uso preventivo do processo de *e-Discovery* está em sua contribuição na mitigação de perdas em decorrência de uma possível ação judicial em razão do tratamento inadequado de informações por parte da organização. Ademais, por não ser economicamente viável adotar um modelo de segurança e armazenamento indiscriminado de todos os dados por um tempo indeterminado, a priorização a partir do *e-Discovery* apontará quais dados são mais críticos do ponto de vista jurídico.

Considerando a publicação das normas ABNT NBR ISO/IEC 27001 e 27002 e as suas versões mais atualizadas de 2013, esta seção apresenta o relacionamento entre os controles de segurança da informação propostos com as etapas do EDRM. A hipótese deste trabalho é que a análise preventiva do uso do modelo EDRM colabora de forma significativa com a identificação de riscos relacionados à segurança da informação. A confiança na efetividade da cobertura/abrangência dos referidos controles de segurança da informação pode ser objetivamente avaliada por meio da perspectiva proporcionada pelo *e-Discovery*. Assim, este

trabalho defende que atuar na gestão dos riscos sob o enfoque do *e-Discovery* contribui para minorar perdas financeiras, econômicas e imagéticas decorrentes de possíveis litígios. Uma organização que tem seu modelo de segurança da informação contraposto ao modelo do *e-Discovery* terá maiores chances de obter as informações necessárias para subsidiar os processos judiciais.

A Norma ABNT 27001:2013 apresenta uma série de controles e objetivos de controles, os quais estão alinhados com aqueles listados na ABNT NBR ISO/IEC 27002:2013, necessários para implementar as opções de tratamento do risco da segurança da informação, os quais são:

- A.5 Políticas de segurança da informação;
- A.6 Organização da segurança da informação;
- A.7 Segurança em recursos humanos;
- A.8 Gestão de ativos;
- A.9 Controle de acesso;
- A.10 Criptografia;
- A.11 Segurança física e do ambiente;
- A.12 Segurança nas operações;
- A.13 Segurança nas comunicações;
- A.14 Aquisição, desenvolvimento e manutenção de sistemas;
- A.15 Relacionamento na cadeia de suprimento;
- A.16 Gestão de incidentes de segurança da informação;
- A.17 Aspectos da segurança da informação na gestão da continuidade do negócio; e
- A.18 Conformidade.

Na Tabela 4.2 é apresentada a proposta quanto ao uso do *e-Discovery* e a sua relação de alto nível com os controles de segurança da informação da norma ISO. As colunas apresentam os vários controles sugeridos pelas Normas ISO 27001:2013 e 27002:2013 para a melhoria contínua da segurança da informação. As linhas apresentam as fases e etapas do EDRM, conforme descrito na Seção 3.2 que trata do modelo de referência para o *e-Discovery* (modelo EDRM). Na interseção entre as linhas e as colunas da Tabela 4.2, buscou-se indicar a existência ou não de possível impacto por parte do *e-Discovery* na priorização, na implantação ou na melhoria dos controles de segurança da informação. Desta maneira, uma organização, interessada em priorizar mecanismos de controle de segurança da informação, pode adotar as

interseções na Tabela 4.2 como indicativo de quais práticas de controle de segurança da informação podem contribuir com o *e-Discovery*. Essa priorização proposta, baseada no *e-Discovery*, colabora na construção de mecanismos de controle de segurança da informação que facilitarão e que darão uma maior agilidade no levantamento de evidências digitais relevantes em casos de litígios.

É importante destacar que a Tabela 4.2 será detalhada, ainda nesta seção, em outras tabelas, de 4.3 a 4.12, que ampliam a visão de quais controles de segurança, específicos da norma ISO 27002:2013, apresentam algum tipo de relação com as etapas do EDRM. As Tabelas 4.2 a 4.12 são acompanhadas de uma descrição quanto às possíveis contribuições entre ambas as partes.

Em relação à fase de Governança da Informação do EDRM, tendo em vista que o modelo apenas aponta para a estrutura conceitual da referida governança, nesta pesquisa decidiu-se adotar artefatos de governança que geralmente são ou deveriam ser utilizados pelas organizações públicas. Foram considerados 03 (três) artefatos de mais alto nível, a saber: Planejamento Estratégico da Organização; Estratégia de Governança Digital - EGD e a Política de Segurança da Informação. Esses três artefatos podem ser considerados como estratégicos para a Governança da Informação, mas necessariamente não precisam estar limitados somente a eles: outros poderão ser incluídos a critério do pesquisador, observando a área de atuação da organização. Especificamente, a Estratégica de Governança Digital foi incluída nos estudos, por se tratar do Decreto nº 8.638, de 15 de janeiro de 2016, que institui a Política de Governança Digital no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional. Para elaboração da EGD foram pesquisados estratégias e documentos de referência no cenário internacional, sendo um deles uma publicação do Conselho da Organização para a Cooperação e Desenvolvimento Econômico (OECD, 2014), que recomendou aos governos desenvolver e implementar estratégias de governo digital que:

> "(...) reflitam uma abordagem de gerenciamento de risco para lidar com as questões de segurança e privacidade digital, e incluam a adoção de medidas eficazes e adequadas de segurança, para aumentar a confiança nos serviços governamentais" (BRASIL, 2016).

Tabela 4.1- Percentual indicativo das fases do EDRM que se relacionam com os controles de segurança da informação

CONTROLES DE SEGURANÇA DA INFORMAÇÃO	A.5 - Política de Segurança da Informação	A.6 - Organização da Segurança da Informação	A.7 - Segurança em Recursos Humanos	A.8 - Gestão de Ativos	A.9 - Controle de Acesso	A.10 - Criptografia	A.11 - Segurança física e do ambiente	A.12 - Segurança nas Operações	A.13 - Segurança nas comunicações	A.14 - Aquisição, Desenvolvimento e Manutenção de sistemas de informação	A.15 - Relacionamento na Cadeia de Suprimento	A.16 - Gestão de Incidentes de segurança da informação	A.17 - Aspectos da segurança da informação na gestão da continuidade do negócio	A.18 - Conformidade
FASES DO MODELO EDRM														
Governança da Informação	100%	67%	33%	67%	33%	33%	0%	33%	33%	33%	33%	33%	33%	33%
Identificação	46%	69%	15%	92%	8%	8%	15%	8%	15%	8%	15%	100%	8%	38%
Preservação	0%	0%	0%	0%	0%	0%	0%	100%	0%	0%	0%	100%	0%	0%
Coleta	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	100%	0%	0%
Processamento	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	100%	0%	0%
Revisão	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	100%	0%	0%
Análise	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	100%	0%	0%
Produção	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	100%	0%	0%
Apresentação	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	100%	0%	0%
PERCENTUAL	20%	24%	7%	30%	4%	4%	4%	15%	7%	4%	7%	96%	4%	13%

Fonte: autor 2016

A Tabela 4.1 apresenta o percentual indicativo das fases do EDRM que se relacionam com os controles de segurança da informação. Esse percentual é o resultado do número de interações encontradas dividido pelo quantitativo total de etapas de cada fase do EDRM, conforme apresentado na Tabela 4.2. Para fins de exemplificação, os 100% presentes entre a fase de Governança da Informação e o controle A.5 – Política de Segurança da Informação na Tabela 4.1 significam que todas as 03 (três) etapas presentes na fase de Governança, a saber, Planejamento Estratégico da Organização, Estratégia de Governança Digital e Política de Segurança da Informação (Tabela 4.2), apresentam relação com o controle A.5 – Política de Segurança da Informação e assim sucessivamente.

A Tabela 4.2, apresenta uma relação de alto nível entre o modelo EDRM e os controles de segurança da informação com as suas devidas observações.

Tabela 4.2 – Relação de alto nível entre o Modelo EDRM e os controles de Segurança da Informação

CONTROLES DE SEGURANÇA DA INFORMAÇÃO	A.5 - Política de Segurança da Informação	A.6 - Organização da Segurança da Informação	A.7 - Segurança em Recursos Humanos	A.8 - Gestão de Ativos	A.9 - Controle de Acesso	A.10 - Criptografia	A.11 - Segurança física e do ambiente	A.12 - Segurança nas Operações	A.13 - Segurança nas comunicações	A.14 - Aquisição, Desenvolvimento e Manutenção de sistemas	A.15 - Relacionamento na Cadeia de Suprimento	A.16 - Gestão de Incidentes de segurança da informação	A.17 - Aspectos da segurança da informação na gestão da continuidade	A.18 - Conformidade
FASES E ETAPAS DO EDRM														
Governança da Informação														
Planejamento Estratégico da Organização	x													
Estratégia de Governança Digital	x	x		x										
Política de Segurança da informação	x	x	x	x	x	x		x	x	x	x	x	x	x
Identificação														
Plano Estratégico de Identifcação de informações relevantes				x								x		
Equipe de Identificação				x								x		
Custodiantes das fontes de informações relevantes		x	x	x	x	x						x		
Intervalo de tempo para busca de informações relevantes				x								x		x
Lista de palavras-chave												x		x
Documentos relevantes e tipos de dados		x		x								x		x
Armazenamento de dados	x	x		x			x					x		x
Sistemas de e-mails	x	x		x					x			x		
Fitas de backup, equipamentos obsoletos e sistemas de Recuperação de Disastres	x	x		x			x	x			x	x	x	x
Inventariar os sistemas legados	x	x		x								x		
Inventariar sistemas armazenados em nuvem ou em terceiros	x	x	x	x					x	x	x	x		
Verificar fontes de recursos adicionais	x	x		x								x		
Apresentar um relatório final com todas as fontes de ESI relevantes		x		x								x		
Preservação														
Desenvolver uma estratégia de preservação de dados								x				x		
Suspender / Elaborar uma tabela para evitar a eliminação de dados importantes								x				x		
Preparar um Plano de Preservação de Dados								x				x		
Selecionar uma metodologia para preservação de dados								x				x		
Executar um Plano de Preservação de dados								x				x		
Coleta														
Desenvolver uma estratégia de coleta de dados												x		
Preparar um Plano de Coleta de Dados												x		
Selecionar uma metodologia para coleta de dados												x		
Executar um Plano de Coleta de dados												x		
Processamento														
Avaliar os dados a serem processados												x		
Realizar a preparação dos dados												x		
Realizar a seleção dos dados												x		
Saída - validação dos dados selecionados												x		
Revisão														
Desenvolver um Plano Estratégico de Revisão												x		
Determinar um local para revisão e treinamento												x		
Desenvolver um fluxo de trabalho e de desempenho												x		
Conduzir a revisão												x		
Avaliar a fase de revisão (Planejado X Executado)												x		
Análise														
Analisar conteúdo e metadados (Gestão da Informação / Pesquisa e Revisão Aprimorada)												x		
Implementar um processo de análise (Análise de Impacto e controle de qualidade)												x		
Produção														
Apresentar formas de produção levantamento de dados												x		
Analisar os registros												x		
Identificar requisitos de produção												x		
Preparar os arquivos												x		
Copiar os arquivos para a media												x		
Apresentação														
Desenvolver uma estratégia de apresentação												x		
Selecionar os formatos de apresentação												x		
Realizar testes de apresentação												x		
Realizar a apresentação perante a Justiça												x		
Arquivar as apresentações e manter histórico												x		

Fonte: autor, 2016

Em uma análise inicial da Tabela 4.2, observa-se que as etapas presentes nas fases de Governança da Informação e de Identificação são as que mais influenciam os controles de segurança da informação das normas ABNT NBR ISO/IEC 27001:2013 e 27002:2013. Há também uma grande interação entre o controle de Gestão de Incidentes de Segurança da Informação e as demais etapas das fases de Preservação, Coleta, Processamento, Revisão, Análise, Produção e Apresentação do modelo EDRM. Destaque para os controles de Política de Segurança da Informação, Organização da Segurança da Informação, Gestão de Ativos e Segurança nas Operações.

É possível depreender da Tabela 4.2 que a etapa Política de Segurança da Informação perpassa por todos os controles de segurança da informação, o que é de certa forma esperado, tendo em vista que a Política de Segurança da Informação deveria abarcar todo o gerenciamento da segurança da informação em uma organização, estabelecendo regras e padrões para proteção da informação. De certa forma, quanto melhor e mais sólida a Política de Segurança da Informação, mais preparada estará a organização para o uso do *e-Discovery*.

As etapas da fase Identificação também apresentam uma grande quantidade de relações com os controles de segurança da informação. Em particular os controles da organização da segurança da informação e gestão de ativos, por estruturarem o gerenciamento da informação, identificar os ativos da organização e definir as devidas responsabilidades pela proteção do ativo.

Verifica-se também que o controle de Gestão de Incidentes de Segurança da Informação tem relação com todas as fases do EDRM. Isso decorre do fato de que esse controle contribui de forma significativa para obtenção de informações digitais relevantes para tratamento de possíveis violações de segurança da informação dentro da própria organização. É de se esperar, portanto, que para tratar das questões de ordem legal/processual, que constitui o caso do uso do *e-Discovery*, o controle Gestão de Incidentes de Segurança da Informação, se implementado adequadamente, em muito contribuirá para a descoberta eletrônica de evidências que possam servir como elemento de prova no processo judicial.

A análise da Tabela 4.2, portanto, permite concluir que a organização que proativamente estabelecer os processos de *e-Discovery* naturalmente estará aprimorando (ou facilitando) a implementação dos controles da norma ISO/IEC 27001:2013. De outra maneira, a organização que optar em fazer uso do modelo EDRM para produção de evidências digitais, obterá vantagens e condições favoráveis para a implementação dos controles de segurança da informação das normas ISO.

As Tabelas 4.3 a 4.12 detalham as relações dos 14 controles de segurança da informação com as fases e etapas do EDRM. Por limitação de espaço e a fim de facilitar a leitura, as tabelas apresentam somente as etapas para as quais identificou-se relação; etapas não apresentadas na tabela, não possuem relação com os controles apontados nas colunas.

Tabela 4.3 - Política de Segurança da Informação e Organização da Segurança da Informação

	5 - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO 6 - ORGANIZAÇÃO DA SEGURANÇA DA INFORMAÇÃO	5.1.1 Políticas para Segurança da Informação	5.1.2 - Análise crítica das políticas para segurança da informação	6.1.1 - Responsabilidades e papéis pela segurança da informação	6.1.2 - Segregação de funções	6.1.3 - Contato com autoridades	6.1.4 - Contato com grupos especiais	6.1.5 - Segurança da informação no gerenciamento de projetos	6.2.1 - Política para o uso de dispositivo móvel	6.2.2 - Trabalho Remoto
FASES E ETAPAS DO EDRM										
GOVERNANÇA DA INFORMAÇÃO										
1	Planejamento Estratégico da Organização	X								
2	Estratégia de Governança Digital	X	X							
3	Política de Segurança da Informação	X	X	X						
IDENTIFICAÇÃO										
1	Plano Estratégico de Identifcação de informações relevantes									
2	Equipe de Identificação									
3	Custodiantes das fontes de informações relevantes			X						
4	Intervalo de tempo para busca de informações relevantes									
5	Lista de palavras-chave									
6	Documentos relevantes e tipos de dados			X			X			
7	Armazenamento de dados	X							X	
8	Sistemas de e-mails	X		X					X	
9	Fitas de backup, equipamentos obsoletos e sistemas de Recuperação de Disastres	X							X	
10	Inventariar os sistemas legados	X		X						
11	Inventariar sistemas armazenados em nuvem ou em terceiros	X		X						X
12	Verificar fontes de recursos adicionais	X		X						
13	Apresentar um relatório final com todas as fontes de ESI relevantes			X						

Fonte: autor, 2016.

Na análise da Tabela 4.3 destaca-se a grande quantidade de interações dos controles 5.1.1 – Políticas para a Segurança da Informação e 6.1.1 – Responsabilidades e papéis pela segurança da informação com as fases de Governança da Informação e Identificação do modelo EDRM, reforçando a hipótese de que a implantação do processo *e-Discovery* produz conhecimento relevante para a implantação ou aprimoramento dos controles de segurança da informação, em particular dos controles 5.1.1 e 6.1.1.

Ainda em relação ao controle 5.1.1 destaca-se a sua relação com as etapas 1, 2 e 3 da Governança de Informação. A norma ISO 27002:2013 sugere que as políticas de segurança da informação contemplem requisitos oriundos da estratégia do negócio; das regulamentações, legislação e contratos; e que seja definido, aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes.

A organização que possuir a política de segurança da informação definida e implementada terá um ponto de partida para atender mais prontamente as etapas 7 a 12 da fase de Identificação do EDRM. A implementação do controle 5.1.1 permite que a organização elabore normativos específicos para tratar as questões de armazenamento de dados, sistema de e-mails, backup, sistema legados, sistemas armazenados em nuvem ou em terceiros e fontes de recursos adicionais.

Quanto ao controle 6.1.1 e sua relação com as fases da Governança da Informação e da Identificação, a norma ISO sugere que a atribuição das responsabilidades pela segurança da informação seja feita em conformidade com as políticas de segurança da informação e que a entidade responsável por cada ativo ou processo de segurança da informação seja determinada e os detalhes dessa responsabilidade sejam documentados. Em resumo, durante o *e-Discovery* é possível avançar mais rapidamente na identificação das fontes de informações, seus responsáveis e principais sistemas correlato quando a organização possui este controle implementado. Além disso, a organização que implementar os processos do e-Discovery terá condições de implementar de forma mais rápida o referido controle.

As demais relações apresentadas na Tabela 4.3 podem indicar contribuição entre o *e-Discovery* e os controles de segurança da informação. O controle 6.1.4 pode prover informações sobre grupos especiais, associações profissionais ou outros fóruns especializados em segurança da informação para ampliar o conhecimento sobre as melhores práticas e manter-se atualizado com as informações relevantes sobre segurança da informação, o que pode colaborar com o processo de *e-Discovery*.

No controle 6.2.1 e sua relação com as etapas 7, 8 e 9 da Identificação, a norma sugere a utilização de dispositivos móveis, sejam tomados cuidados especiais para assegurar que as informações do negócio não sejam comprometidas, que a política de dispositivos móveis leve em consideração os riscos de se trabalhar com esses dispositivos móveis em ambientes desprotegidos e que considerem assim como o modelo EDRM, o backup, as informações armazenadas em dispositivos móveis e o uso de e-mail nesses dispositivos, que podem não ser passíveis de cópia de segurança.

Tabela 4.4 -Segurança em Recursos Humanos

	7 - SEGURANÇA EM RECURSOS HUMANOS	7.1.1 - Seleção	7.1.2 - Termos e Condições de Contratação	7.2.1 - Responsabilidades da Direção	7.2.2 - Conscientização, educação e treinamento em segurança da informação	7.2.3 - Processo disciplinar	7.3.1 - Responsabilidades pelo encerramento ou mudança da contratação
FASES E ETAPAS DO EDRM							
GOVERNANÇA DA INFORMAÇÃO							
1	Planejamento Estratégico da Organização						
2	Estratégia de Governança Digital						
3	Política de Segurança da Informação		**X**				
IDENTIFICAÇÃO							
1	Plano Estratégico de Identifcação de informações relevantes						
2	Equipe de Identificação						
3	Custodiantes das fontes de informações relevantes			**X**			**X**
4	Intervalo de tempo para busca de informações relevantes						
5	Lista de palavras-chave						
6	Documentos relevantes e tipos de dados						
7	Armazenamento de dados						
8	Sistemas de e-mails						
9	Fitas de backup, equipamentos obsoletos e sistemas de Recuperação de Disastres						
10	Inventariar os sistemas legados						
11	Inventariar sistemas armazenados em nuvem ou em terceiros		**X**				
12	Verificar fontes de recursos adicionais						
13	Apresentar um relatório final com todas as fontes de ESI relevantes						

Fonte: autor, 2016.

Na análise da Tabela 4.4 destaca-se o controle 7.1.2 – Termos e Condições de Contratação, com duas marcações, uma na etapa Política de Segurança da Informação, da fase de Governança da Informação, e outra na etapa inventariar sistemas armazenados em nuvem ou em terceiros, da fase de Identificação. No que tange a este controle, a norma sugere que as obrigações contratuais para funcionários e partes externas reflitam as políticas para segurança da informação da organização e que se esclareça e declare todos os funcionários, fornecedores e partes externas que tenham acesso às informações sensíveis e que assinem um termo de confidencialidade ou de não divulgação, antes de lhes ser dado o acesso aos recursos de processamento da informação. Em se considerando o e-Discovery, caso este esteja implementado, permiti que os advogados apresentem perante a justiça evidências que os funcionários e as empresas terceirizadas conheciam as políticas de segurança da informação, o que pode ser relevante para caso de vazamento de informações sensíveis de uma organização, bem como para tratar de outras questões de ordem jurídica.

Já no controle 7.2.1, e a sua relação com etapa 2 da fase de identificação, a norma sugere que a direção da organização solicite a todos os funcionários e partes externas que pratiquem a segurança da informação de acordo com o estabelecido nas políticas e procedimentos da organização. Ademais, é esperado que, antes de obter acesso às informações sensíveis ou aos sistemas de informação, os funcionários estejam adequadamente instruídos sobre as suas responsabilidades e papéis pela segurança da informação. Portanto, se a organização possui um registro de quais informações ou sistemas são sensíveis e quem tem acesso a eles, o modelo EDRM pode valer-se de tais registros para prontamente identificar os custodiantes das fontes de informações relevantes. Importante destacar que se os funcionários e fornecedores não forem conscientizados sobre as suas responsabilidades quanto à segurança da informação, eles podem alegar em juízo que não foram instruídos da sensibilidade da informação.

Em relação ao controle 7.3.1 e à sua relação com a etapa 2 da Identificação, a norma sugere que as mudanças de responsabilidades ou do trabalho sejam gerenciadas quando ocorrer o encerramento da responsabilidade ou do trabalho atual, combinado com o início de novas responsabilidades ou trabalho. O correto registro das mudanças supramencionadas permite manter a cadeia dos custodiantes das fontes de informações relevantes atualizada, o que em muito facilitará esta etapa do processo de descoberta eletrônica.

Tabela 4.5 - Gestão de Ativos

	8 - GESTÃO DE ATIVOS	8.1.1 - Inventário dos ativos	8.1.2 - Proprietário dos ativos	8.1.3 - Uso aceitável dos ativos	8.1.4 - Devolução de ativos	8.2.1 - Classificação da Informação	8.2.2 - Rótulos e tratamento da informação	8.2.3 - Tratamento dos ativos	8.3.1 - Gerenciamento de mídias removíveis	8.3.2 - Descarte de mídias	8.3.3 - Transferência física de mídias
FASES E ETAPAS DO EDRM											
GOVERNANÇA DA INFORMAÇÃO											
1	Planejamento Estratégico da Organização										
2	Estratégia de Governança Digital					X					
3	Política de Segurança da Informação					X					
IDENTIFICAÇÃO											
1	Plano Estratégico de Identifcação de informações relevantes	X				X					
2	Equipe de Identificação	X									
3	Custodiantes das fontes de informações relevantes	X	X			X					
4	Intervalo de tempo para busca de informações relevantes					X					
5	Lista de palavras-chave										
6	Documentos relevantes e tipos de dados						X				
7	Armazenamento de dados							X			
8	Sistemas de e-mails				X						
9	Fitas de backup, equipamentos obsoletos e sistemas de Recuperação de Disastres				X				X	X	X
10	Inventariar os sistemas legados				X						
11	Inventariar sistemas armazenados em nuvem ou em terceiros				X						
12	Verificar fontes de recursos adicionais			X							
13	Apresentar um relatório final com todas as fontes de ESI relevantes	X									

Fonte: autor, 2016.

Na análise da Tabela 4.5 destacam-se os controles 8.1.1 – Inventários dos ativos; 8.1.4 – Devolução de ativos e 8.2.1 – Classificação da Informação, ambos com a maioria das marcações na fase de Identificação do EDRM.

Quantos ao controle 8.1.1 e 8.1.2 e suas relações com as etapas 1, 2, 3 e 13 da fase de Identificação, a norma sugere preparar um plano de identificação que esteja em conformidade com o objetivo da organização de identificar os ativos relevantes e documentar a sua importância. Que se constitua uma equipe interna ou externa da organização que se ocupará em realizar a identificação dos ativos relevantes. A norma também sugere que para cada ativo identificado seja indicado um responsável, que seja apresentado um inventário de ativos que seja completo, atualizado, consistente e alinhado com outros inventários e que os ativos mantidos no inventário tenham um proprietário. Essas sugestões da norma estão alinhadas com as etapas do EDRM, que prevê a elaboração de um plano estratégico de identificação de informações relevantes, que seja formada uma equipe de identificação para distinguir os custodiantes de informações relevantes, e que por fim apresente um relatório final com todas as fontes de ESI relevantes.

No controle 8.1.3 e a sua relação com a etapa 12 da fase de Identificação, a norma sugere que regras para o uso aceitável das informações, dos ativos associados com a informação e dos recursos de processamento da informação, sejam identificadas, documentadas e implementadas. Neste sentido, as regras devem estabelecer critérios para que recursos externos possam ser utilizados para acesso à sua rede de dados. Por exemplo: computadores/notebooks pessoais, dispositivos móveis, smartphones, armazenamento em nuvem, acessos remotos, etc. Esses recursos devem ser considerados durante a etapa 12 da fase de Identificação, de modo que, se o controle 8.1.3 for existente, é facilitado o trabalho da equipe de descoberta eletrônica.

No controle 8.1.4 e a sua relação com as etapas 8 a 11 da fase de Identificação, no controle busca-se garantir que todos os funcionários e partes externas devolvam todos os ativos da organização que estejam em sua posse, após o encerramento de suas atividades, do contrato ou acordo. Nessa etapa do EDRM é realizado um questionamento similar. Observa-se que a implementação deste controle por parte da organização pode trazer outras facilidades ao processo, uma vez que a norma também sugere sobre controles que, se não implementados, podem expor juridicamente a organização. Como exemplo considere os seguintes cenários:

- Em caso do funcionário ou parte externa adquira o equipamento da organização, que se elaborem procedimentos para assegurar que toda a informação relevante

seja transferida para a organização e seja apagada de forma segura do equipamento.

- Que, durante o período de encerramento de atividades, a organização monitore possíveis cópias de informações relevantes (por exemplo, propriedade intelectual) pelos funcionários ou partes externas que estão saindo da organização.

Esses controles também podem ser encontrados dispersos em diferentes etapas da fase de identificação.

No controle 8.2.1 e sua relação com as etapas 2 e 3 da Governança da Informação, é importante destacar que, para órgãos públicos, a EGD se compromete com a classificação de dados como abertos e transparentes, ressalvado o disposto em contrário em legislação específica. A norma sugere que o esquema de classificação inclua convenções para classificação e critérios para análise crítica da classificação ao longo do tempo; que o nível de proteção seja avaliado por meio da análise da confidencialidade, integridade e disponibilidade, e de quaisquer requisitos considerados para a informação. E que o esquema de classificação esteja alinhado com a política de controle de acesso. Em relação às etapas 1, 3 e 4 da fase de Identificação, a norma sugere que a classificação e os controles de proteção, associados à informação, levem em consideração as necessidades do negócio em compartilhar ou restringir a informação bem como os requisitos legais. Ela também sugere que os proprietários de ativos de informação sejam responsáveis por sua classificação e que o esquema de classificação inclua convenções para classificação e critérios para análise crítica da classificação ao longo do tempo.

No controle 8.2.2 e sua relação com a etapa 6 da Identificação, a norma sugere um conjunto apropriado de procedimentos para rotular e tratar a informação, que seja desenvolvido e implementado de acordo com o esquema de classificação da informação adotado pela organização. A classificação dos dados, se implementadas por este controle, também colabora com a fase de identificação do EDRM.

Quanto aos controles 8.3.1, 8.3.2 e 8.3.3 e às suas relações com a etapa 9 da Identificação, a norma sugere um conjunto de subcontroles que estão perfeitamente alinhados com os objetivos da etapa 9 que trata de backup, equipamentos obsoletos e sistemas de recuperação de desastres. São recomendações da norma:

- prevenir a divulgação não autorizada, modificação, remoção ou destruição da informação armazenada nas mídias;

- que as mídias sejam descartadas de forma segura, quando não forem mais necessárias, por meio de procedimentos formais. Equipamentos danificados contendo dados sensíveis podem exigir uma avaliação de riscos para determinar se é recomendado que os itens sejam destruídos fisicamente em vez de serem enviados para conserto ou descartados; e
- que as mídias contendo informações sejam protegidas contra acesso não autorizado, uso impróprio ou corrupção, durante o transporte.

Tabela 4.6 - Controle de Acesso e Criptografia

	9 - CONTROLE DE ACESSO 10 - CRIPTOGRAFIA	9.1.1 - Política de Controle de Acesso	9.2.1 - Registro e cancelamento de usuário	9.2.2 - Provisionamento para acesso de usuário	9.2.3 - Gerenciamento de direitos de acesso privilegiados	9.2.4 - Gerenciamento da informação de autenticação secreta de usuários	9.2.5 - Análise crítica dos direitos de acesso de usuário	9.3.1 - Uso da Informação de autenticação secreta	9.4.1 - Restrição de acesso à Informação	9.4.2 - Procedimentos seguros de entrada no sistema (log-on)	9.4.3 - Sistema de gerenciamento de senha	9.4.4 - Uso de programas utilitários privilegiados	9.4.5 - Controle de acesso ao código-fonte de programas	10.1.1 - Política para o uso de controles criptográficos	10.1.2 - Gerenciamento de chaves
FASES E ETAPAS DO EDRM															
GOVERNANÇA DA INFORMAÇÃO															
1	Planejamento Estratégico da Organização														
2	Estratégia de Governança Digital														
3	Política de Segurança da Informação	X	X	X	X	X	X	X	X	X	X	X	X	X	
IDENTIFICAÇÃO															
1	Plano Estratégico de Identifcação de informações relevantes														
2	Equipe de Identificação														
3	Custodiantes das fontes de informações relevantes	X	X	X	X	X	X	X	X	X	X	X	X	X	
4	Intervalo de tempo para busca de informações relevantes														
5	Lista de palavras-chave														
6	Documentos relevantes e tipos de dados														
7	Armazenamento de dados														
8	Sistemas de e-mails														
9	Fitas de backup, equipamentos obsoletos e sistemas de Recuperação de Disastres														
10	Inventariar os sistemas legados														
11	Inventariar sistemas armazenados em nuvem ou em terceiros														
12	Verificar fontes de recursos adicionais														
13	Apresentar um relatório final com todas as fontes de ESI relevantes														

Fonte: autor, 2016.

Na análise da Tabela 4.6 destacam-se todos os subcontroles relacionados ao controle de acesso. Isto porque as informações prestadas por tais controles são relevantes no contexto da descoberta eletrônica. Ao EDRM interessa ainda conhecer os usuários autorizados ou não a fazer determinados tipos de acesso, e como tais privilégios mudaram no decorrer do tempo.

Quanto ao controle 10.1.1 e sua relação com a etapa 3 da fase de Identificação, a norma sugere que seja desenvolvida e implementada uma política sobre o uso de controles criptográficos para a proteção da informação, o que também interessa à descoberta eletrônica, uma vez que informações criptografadas não podem ser descobertas.

Tabela 4.7 - Segurança Física do Ambiente

	11 - SEGURANÇA FÍSICA DO AMBIENTE	11.1.1 - Perímetro de segurança física	11.1.2 - Controles de entrada física	11.1.3 - Segurança em escritórios, salas e instalações	11.1.4 - Proteção contra ameaça externas e do meio ambiente	11.1.5 - Trabalhando em áreas seguras	11.1.6 - Áreas de entrega e de carregamento	11.2.1 - Localização e proteção do equipamento	11.2.2 - Utilidades	11.2.3 - Segurança do cabeamento	11.2.4 - Manutenção dos equipamentos	11.2.5 - Remoção de ativos	11.2.6 - Segurança de equipamentos e ativos fora das dependências da	11.2.7 - Reutilização ou descarte seguro de equipamentos	11.2.8 - Equipamento de usuário sem monitoração	11.2.9 - Política de mesa limpa e tela limpa
FASES E ETAPAS DO EDRM																
GOVERNANÇA DA INFORMAÇÃO																
1	Planejamento Estratégico da Organização															
2	Estratégia de Governança Digital															
3	Política de Segurança da Informação															
IDENTIFICAÇÃO																
1	Plano Estratégico de Identifcação de informações relevantes															
2	Equipe de Identificação															
3	Custodiantes das fontes de informações relevantes															
4	Intervalo de tempo para busca de informações relevantes															
5	Lista de palavras-chave															
6	Documentos relevantes e tipos de dados															
7	Armazenamento de dados													**X**		
8	Sistemas de e-mails															
9	Fitas de backup, equipamentos obsoletos e sistemas de Recuperação de Disastres													**X**		
10	Inventariar os sistemas legados															
11	Inventariar sistemas armazenados em nuvem ou em terceiros															
12	Verificar fontes de recursos adicionais															
13	Apresentar um relatório final com todas as fontes de ESI relevantes															

Fonte: autor, 2016.

Na análise da Tabela 4.7 fica evidenciado que o EDRM não trata de forma explícita a segurança física do ambiente organizacional. Por esse motivo não se verificam relações na Tabela 4.7.

Este trabalho considerou o controle 11.2.7 relevante pois trata da reutilização ou descarte seguro de equipamentos em que é preciso assegurar que todos os dados sensíveis, softwares com credenciais de acesso remoto sejam devolvidos, destruídos ou sobrescritos.

Os controles de segurança física do ambiente podem ser considerados como possível acréscimo ao EDRM, pois informações relevantes em determinados casos podem ser relacionadas a violações físicas e não lógicas.

Tabela 4.8 - Segurança nas Operações

	12 - SEGURANÇA NAS OPERAÇÕES	12.1.1 - Documentação dos procedimentos de operação	12.1.2 - Gestão de Mudanças	12.1.3 - Gestão de Capacidades	12.1.4 - Separação dos ambientes de desenvolvimento, teste e	12.2.1 - Controle contra malware	12.3.1 - Cópias de segurança das informações	12.4.1 - Registro de eventos	12.4.2 - Proteção das informações dos registros de eventos (logs)	12.4.3 - Registros de eventos (log) de administrador e operador	12.4.4 - Sincronização dos relógios	12.5.1 - Instalação de software nos sistemas operacionais	12.6.1 - Gestão de vulnerabilidades técnicas	12.6.2 - Restrições quanto à instalação de software	12.7.1 - Controles de auditoria de sistemas de informação
FASES E ETAPAS DO EDRM															
GOVERNANÇA DA INFORMAÇÃO															
1	Planejamento Estratégico da Organização														
2	Estratégia de Governança Digital														
3	Política de Segurança da Informação						X								X
IDENTIFICAÇÃO															
1	Plano Estratégico de Identifcação de informações relevantes														
2	Equipe de Identificação														
3	Custodiantes das fontes de informações relevantes														
4	Intervalo de tempo para busca de informações relevantes														
5	Lista de palavras-chave														
6	Documentos relevantes e tipos de dados														
7	Armazenamento de dados														
8	Sistemas de e-mails														
9	Fitas de backup, equipamentos obsoletos e sistemas de Recuperação de Disastres	X													
10	Inventariar os sistemas legados														
11	Inventariar sistemas armazenados em nuvem ou em terceiros														
12	Verificar fontes de recursos adicionais														
13	Apresentar um relatório final com todas as fontes de ESI relevantes														
PRESERVAÇÃO															
1	Desenvolver uma estratégia de preservação de dados						X	X	X	X					
2	Suspender / Elaborar uma tabela para evitar a eliminação de dados importantes						X	X	X	X					
3	Preparar um Plano de Preservação de Dados						X	X	X	X					
4	Selecionar uma metodologia para preservação de dados						X	X	X	X					
5	Executar um Plano de Preservação de dados						X	X	X	X					

Fonte: autor, 2016.

Na análise da Tabela 4.8 destaca-se o controle 12.1.1 e a sua relação com a etapa 9 da fase de Identificação. Para o modelo EDRM, o sistema de backup é muito utilizado no processo de descoberta eletrônica, tendo em vista que para atender às demandas judiciais, pode ser necessário recuperar informações que já foram arquivadas. A norma recomenda que a organização estabeleça uma política de backup para definição dos requisitos relativos às cópias de segurança das informações, dos softwares e dos sistemas, o que justifica a relação indicada entre o controle 12.1.1 e a etapa 9 supramencionada.

Nessa tabela outros controles também são destacados, como: 12.3.1 – Cópias de segurança das informações, 12.4.1 – Registro de eventos, 12.4.2 - Proteção das informações dos registros de eventos (logs) e 12.4.3 - Registros de eventos (log) de administrador e operador. Esses controles se relacionam com as etapas 1, 2, 3, 4 e 5 da fase de Preservação, a saber: desenvolver uma estratégia de preservação de dados, suspender/elaborar uma tabela para evitar a eliminação de dados importantes, preparar um plano de preservação de dados, selecionar um modelo para preservação de dados e executar um plano de preservação de dados.

Os controles supracitados têm relação nas etapas da fase de Preservação do EDRM, pois a norma ABNT sugere que cópias de segurança das informações, dos softwares e das imagens do sistema sejam efetuadas e testadas regularmente. Além disso, a norma também recomenda que os registros (log) de eventos das atividades do usuário, administradores e operadores de sistemas, exceções, falhas e eventos de segurança da informação sejam produzidos, mantidos e analisados criticamente, a intervalos regulares. Ou seja, esses controles contribuem para a preservação de informações que poderão ser relevantes no decorrer do processo de descoberta eletrônica.

Quanto ao controle 12.7.1 destaca-se a sua relação com a etapa 3 da fase de Identificação, pois a norma sugere que sejam planejados e acordados requisitos de auditoria envolvendo a verificação nos sistemas operacionais para minimizar a interrupção dos processos do negócio. Portanto, a inclusão de auditoria na Política de Segurança da Informação está alinhada com o modelo de EDRM, como também com a hipótese trabalhada nesta pesquisa, uma vez que ao se preparar para realizar descobertas eletrônicas por meio do EDRM, uma organização estará produzindo material que pode servir como instrumento de investigação/auditoria interna.

Tabela 4.9 - Segurança nas Comunicações

	13 - SEGURANÇA NAS COMUNICAÇÕES	13.1.1 - Contoles de redes	13.1.2 - Segurança dos serviços de rede	13.1.3 - Segregação de redes	13.2.1 - Políticas e procedimentos para transferência de informações	13.2.2 - Acordos para transferência de informações	13.2.3 - Mensagens eletrônicas	13.2.4 - Acordos de confidencialidade e não divulgação
FASES E ETAPAS DO EDRM								
GOVERNANÇA DA INFORMAÇÃO								
1	Planejamento Estratégico da Organização							
2	Estratégia de Governança Digital							
3	Política de Segurança da Informação				**X**			**X**
IDENTIFICAÇÃO								
1	Plano Estratégico de Identifcação de informações relevantes							
2	Equipe de Identificação							
3	Custodiantes das fontes de informações relevantes							
4	Intervalo de tempo para busca de informações relevantes							
5	Lista de palavras-chave							
6	Documentos relevantes e tipos de dados							
7	Armazenamento de dados							
8	Sistemas de e-mails						**X**	
9	Fitas de backup, equipamentos obsoletos e sistemas de Recuperação de Disastres							
10	Inventariar os sistemas legados							
11	Inventariar sistemas armazenados em nuvem ou em terceiros							**X**
12	Verificar fontes de recursos adicionais							
13	Apresentar um relatório final com todas as fontes de ESI relevantes							

Fonte: autor, 2016.

Na análise da Tabela 4.9 destacam-se os controles 13.2.1 – Políticas e procedimentos para transferência de informações, 13.2.3 - Mensagens eletrônicas e 13.2.4 – Acordos de confidencialidade e não divulgação. Esses controles relacionam com as fases de Governança da Informação e Identificação do EDRM.

O controle 13.2.1 se relaciona com a etapa 3 da Governança da Informação, tendo em vista que a norma recomenda que políticas, procedimentos e controles de transferências formais sejam estabelecidos para proteger a transferência de informações, por meio do uso de todos os tipos de recursos de comunicação. Ou seja, a organização que faça constar em seu regramento sobre a Política de Segurança da Informação, questões relacionadas à proteção quanto à transferência de informações, poderá descobrir violações que causem a quebra de segurança da informação, de forma mais sistematizada que uma organização que não tenha esse controle implementado.

Quanto ao controle 13.2.3 e sua relação com a etapa 8 da Identificação, a norma sugere que as informações que trafegam em mensagens eletrônicas sejam adequadamente protegidas. Nesse sentido, o controle está alinhado com o EDRM quando trata da questão do permissionamento ao acesso remoto e ao armazenamento de e-mails da organização, independentemente dos dispositivos de armazenamento ou localização.

Em se tratando do controle 13.2.4 e a sua relação com a etapa 3 da Governança da Informação e com a etapa 11 da Identificação, a norma recomenda que os acordos de confidencialidade e de não divulgação considerem os requisitos para proteger as informações confidenciais, usando termos que são obrigados do ponto de vista legal. Os acordos de confidencialidade ou não divulgação são aplicáveis às partes externas ou aos funcionários da organização. Do ponto de vista do *e-Discovery*, a organização que se preocupa em proteger as informações por meio de acordos de confidencialidade ou não divulgação, estará se precavendo quanto a futuros problemas judiciais.

Portanto, a implementação preventiva do processo de *e-Discovery* corrobora com a priorização dos controles supramencionados, resguardando a organização com as informações que podem ser relevantes no litígio que envolva transferência de informações, acordo de confidencialidade e troca de mensagens eletrônicas.

Tabela 4.10 -Aquisição, Desenvolvimento e Manutenção de Sistemas

	14 - AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS	14.1.1 - Análise e especificação dos requisitos de segurança da informação	14.1.2 - Serviços de aplicação seguros em redes públicas	14.2.1 - Política de desenvolvimento seguro	14.2.2 - Procedimentos para controle de mudanças de sistemas	14.2.3 - Análise crítica técnica das aplicações após mudanças nas plataformas operacionais	14.2.4 - Restriçoes sobre mudanças em pacotes de software	14.2.5 - Princípios para projetar sistemas seguros	14.2.6 - Ambiente seguro para desenvolvimento	14.2.7 - Desenvolvimento terceirizado	14.2.8 - Teste de segurança do sistema	14.2.9 - Teste de aceitação de sistemas	14.3.1 - Proteção dos dados para teste
FASES E ETAPAS DO EDRM													
GOVERNANÇA DA INFORMAÇÃO													
1	Planejamento Estratégico da Organização												
2	Estratégia de Governança Digital												
3	Política de Segurança da Informação			X									
IDENTIFICAÇÃO													
1	Plano Estratégico de Identifcação de informações relevantes												
2	Equipe de Identificação												
3	Custodiantes das fontes de informações relevantes												
4	Intervalo de tempo para busca de informações relevantes												
5	Lista de palavras-chave												
6	Documentos relevantes e tipos de dados												
7	Armazenamento de dados												
8	Sistemas de e-mails												
9	Fitas de backup, equipamentos obsoletos e sistemas de Recuperação de Disastres												
10	Inventariar os sistemas legados												
11	Inventariar sistemas armazenados em nuvem ou em terceiros									X			
12	Verificar fontes de recursos adicionais												
13	Apresentar um relatório final com todas as fontes de ESI relevantes												

Fonte: autor, 2016.

Na análise da Tabela 4.10 destacam-se os controles 14.2.1 – Políticas de desenvolvimento seguro e 14.2.7 – Desenvolvimento terceirizado das fases de Governança da Informação e Identificação.

No controle 14.2.1 e sua relação com a etapa 3 da fase de Governança da Informação, a norma sugere regras para o desenvolvimento de sistemas e software sejam estabelecidas e aplicadas aos desenvolvimentos realizados dentro da organização.

No controle 14.2.7 e sua relação com a etapa 11 da fase de Identificação, a norma sugere que a organização supervisione e monitore as atividades de desenvolvimento de sistemas terceirizados.

Ambos os controles, se implementados, facilitam o uso do processo de descoberta eletrônica nas organizações, pois incentivam a elaboração de políticas de segurança específicas para aquisição, desenvolvimento e manutenção segura de suas aplicações com a supervisão e monitoramento dos terceirizados. Portanto, organizações que tenham preocupação com a preservação de evidências que possam estar relacionadas a violações de segurança da informação relacionados à terceirização de desenvolvimento e manutenção de sistemas, devem priorizar a implementação desses controles, uma vez que eles contribuem para a descoberta eletrônica em eventuais litígios.

Um exemplo de área de contestação judicial é a disputa por propriedade intelectual entre contratante e contratada.

Tabela 4.11 - Relacionamento na Cadeia de Suprimento e Gestão de Incidentes de Segurança da Informação

	15 - RELACIONAMENTO NA CADEIA DE SUPRIMENTO 16 - GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO	15.1.1 - Política de seg. da inf. no relacionamento com os fornecedores	15.1.2 - Identificando segurança da informação nos acordos com fornecedores	15.1.3 - Cadeia de suprimento na tecnologia da informação e comunicação	15.2.1 - Monitoramento e análise crítica de serviços com fornecedores	15.2.2 - Gerenciamento de mudanças para serviços com fornecedores	16.1.1 - Responsabilidade e procedimentos	16.1.2 - Notificação de eventos de segurança da informação	16.1.3 - Notificando fragilidades de segurança da informação	16.1.4 - Avaliação e decisão dos eventos de segurança da informação	16.1.5 - Resposta aos incidentes de segurança da informação	16.1.6 - Aprendendo com os incidentes de segurança da informação	16.1.7 - Coleta de evidências
FASES E ETAPAS DO EDRM													
GOVERNANÇA DA INFORMAÇÃO													
1	Planejamento Estratégico da Organização												
2	Estratégia de Governança Digital												
3	Política de Segurança da Informação	X											X
IDENTIFICAÇÃO													
1	Plano Estratégico de Identifcação de informações relevantes												X
2	Equipe de Identificação												X
3	Custodiantes das fontes de informações relevantes						X						X
4	Intervalo de tempo para busca de informações relevantes												X
5	Lista de palavras-chave												X
6	Documentos relevantes e tipos de dados												X
7	Armazenamento de dados												X
8	Sistemas de e-mails												X
9	Fitas de backup, equipamentos obsoletos e sistemas de Recuperação de Disastres				X								X
10	Inventariar os sistemas legados												X
11	Inventariar sistemas armazenados em nuvem ou em terceiros		X		X								X
12	Verificar fontes de recursos adicionais												X
13	Apresentar um relatório final com todas as fontes de ESI relevantes												X
PRESERVAÇÃO													
1	Desenvolver uma estratégia de preservação de dados												X
2	Suspender / Elaborar uma tabela para evitar a eliminação de dados importantes												X
3	Preparar um Plano de Preservação de Dados												X
4	Selecionar uma metodologia para preservação de dados												X
5	Executar um Plano de Preservação de dados												X
COLETA													
1	Desenvolver uma estratégia de coleta de dados												X
2	Preparar um Plano de Coleta de Dados												X
3	Selecionar uma metodologia para coleta de dados												X
4	Executar um Plano de Coleta de dados												X
PROCESSAMENTO													
1	Avaliar os dados a serem processados												X
2	Realizar a preparação dos dados												X
3	Realizar a seleção dos dados												X
4	Saída - validação dos dados selecionados												X
REVISÃO													
1	Desenvolver um Plano Estratégico de Revisão												X
2	Determinar um local para revisão e treinamento												X
3	Desenvolver um fluxo de trabalho e de desempenho												X
4	Conduzir a revisão												X
5	Avaliar a fase de revisão (Planejado X Executado)												X
ANÁLISE													
1	Analisar conteúdo e metadados (Gestão da Informação / Pesquisa e Revisão Aprimorada)												X
2	Implementar um processo de análise (Análise de Impacto e controle de qualidade)												X
PRODUÇÃO													
1	Apresentar formas de produção levantamento de dados												X
2	Analisar os registros												X
3	Identificar requisitos de produção												X
4	Preparar os arquivos												X
5	Copiar os arquivos para a media												X
APRESENTAÇÃO													
1	Desenvolver uma estratégia de apresentação												X
2	Selecionar os formatos de apresentação												X
3	Realizar testes de apresentação												X
4	Realizar a apresentação perante a Justiça												X
5	Arquivar as apresentações e manter histórico												X

Fonte: autor, 2016.

No que tange ao relacionamento na cadeia de suprimentos sugeridos pelas normas ABNT NBR ISO/IEC 27001 e 27002:2013, aplicam-se os mesmos princípios apresentados para os controles relacionados à aquisição, desenvolvimento e manutenção de sistemas, tendo em vista tratar-se de terceirização e dos riscos associados.

Na análise da Tabela 4.11 destaca-se o controle 15.1.1 e a sua relação com a etapa 3 da fase de Identificação. A norma recomenda que os requisitos de segurança da informação, para diminuir os riscos associados com o acesso dos fornecedores aos ativos da organização, sejam acordados com o fornecedor e documentados. Esse controle tem como proposta manter uma política de segurança da informação no relacionamento com os fornecedores, fortalecendo assim a fase de governança da informação do EDRM.

Quanto ao controle 15.1.2 e a sua relação com a etapa 11 da fase de Identificação, a norma recomenda que um processo para identificação dos componentes do serviço ou produto, que são críticos para a organização, necessitam de uma maior atenção e verificação quando construídos fora da organização, especialmente se o fornecedor principal terceirizar parte dos componentes do serviço ou produto com outros fornecedores. Esse controle tem como proposta identificar os quesitos de segurança da informação nos acordos com fornecedores, que pode facilitar a descoberta eletrônica na etapa de inventariar sistemas armazenados em nuvem ou em terceiros do EDRM.

Em se tratando do controle 15.2.1 e a sua relação com as etapas 9 e 11 da fase de Identificação, a norma recomenda que o fornecedor mantenha capacidade de serviço suficiente em conjunto com planos de trabalho desenhados, para assegurar que os níveis de continuidade do serviço acordados sejam mantidos, no caso de um desastre ou falha dos serviços principais. Se implementado, este controle permite à equipe de descoberta eletrônica maior acesso ao universo das informações de auditorias independentes, sobre incidentes de segurança da informação ou problemas relativos às falhas por serviços prestados por terceiros.

Quanto à Gestão de Incidentes de Segurança da Informação no que se refere ao controle 16.1.1 e à sua relação com a etapa 3 da fase de Identificação, a norma recomenda que responsabilidades e procedimentos de gestão sejam estabelecidos para assegurar respostas rápidas, efetivas e ordenadas aos incidentes de segurança da informação. Esse controle pode corroborar com o trabalho de descoberta eletrônica, pois a equipe de tratamento de incidentes de segurança da informação poderá trabalhar em conjunto com os custodiantes das informações para verificar quais alterações ou anomalias foram detectadas em um determinado sistema.

No controle 16.1.7 e as suas relações com as etapas 3 da fase de Governança da Informação e 6 da fase Identificação, a norma recomenda que a organização defina e aplique procedimentos para a identificação, coleta, aquisição e preservação das informações, as quais podem servir como evidências. Considera-se que esse controle interaja com a Política de Segurança da Informação e influencie principalmente na identificação de documentos potencialmente relevantes e nos tipos de dados do EDRM. A norma ISO 27002:2013 ainda cita que a identificação é o processo envolvendo a busca, reconhecimento e documentação de potencial evidência.

Ainda sobre o controle 16.1.17, sua relação se mantém presente nas fases da Identificação, Preservação, Coleta e Processamento, principalmente porque esse controle remete à norma ABNT ISO/IEC 27037:2013 que fornece diretrizes para identificação, coleta, aquisição e preservação de evidências digitais. Quanto às etapas das fases de Revisão, Análise, Produção e Apresentação, essas foram assinaladas na tabela por terem relação direta com os objetivos apresentados pelo controle 16.1.17 do Sistema de Gestão de Segurança da Informação de uma organização. Isto significa dizer que tanto o SGSI quanto o EDRM trabalham com a identificação, preservação, coleta, processamento, revisão, análise, produção e apresentação de evidências, embora com diferenças de enfoque. O primeiro sob enfoque de incidentes, e o segundo sob enfoque de descoberta eletrônica para apresentação perante a justiça ou órgãos de controle.

Cabe ressaltar que podem existir situações em que o trabalho da equipe de tratamento de incidentes de segurança da informação pode ser disputado pela outra parte do processo, ou então, que não seja suficiente para levantar as informações relevantes por parte do *e-Discovery*, bem como para validar as evidências digitais perante a Justiça. Casos assim podem exigir a participação de peritos em forense digital que trabalham com softwares e processos especializados, bem como o atestado profissional de quem é capacitado para a realização de atividades de perícias digitais.

Para Eleutério e Machado (2011) o objetivo da computação forense está em determinar a dinâmica e a materialidade de ilícitos relacionados à área da informática. Isso ocorre com a utilização de técnicas e métodos científicos, com o foco principal na identificação e análise do processo das evidências digitais e matérias de crime. A forense digital se torna imprescindível quando as disputas judiciais envolvem questões relacionadas à propriedade intelectual, crimes cibernéticos, danos significativos (financeiros ou imagem), disputas trabalhistas ou fraudes, que por meio do laudo pericial apresenta, de forma imparcial, o que foi possível identificar da

dinâmica, materialidade e autoria do fato apurado, sendo relacionados com os princípios da forense digital apresentado por Casey (2011), a saber: troca de evidência, características da evidência, respeito aos preceitos forenses, autenticação, cadeia de custódia, integridade da evidência, objetividade e repetível.

Tabela 4.12 - Aspectos da Segurança da Informação na Gestão da Continuidade do Negócio e Conformidade

	17 - Aspectos da segurança da informação na gestão da continuidade do negócio 18 - Conformidade	17.1.1 - Planejando a continuidade da segurança da informação	17.1.2 - Implementando a continuidade da segurança da informação	17.1.3 - Verificação, análise crítica e avaliação da continuidade da segurança da	17.2.1 - Disponibilidade dos recursos de processamento da informação	18.1.1 - identificação da legislação aplicável e de requisitos contratuais	18.1.2 - Direitos de propriedade intelectual	18.1.3 - Proteção de registros	18.1.4 - Proteção e privacidade de informações de identificação pessoal	18.1.5 - Regulamentação de controles de criptografia	18.2.1 - Análise crítica independente da segurança da informação	18.2.2 - Conformidade com as políticas e procedimentos de segurança da informação	18.2.3 - Análise crítica da conformidade técnica
FASES E ETAPAS DO EDRM													
GOVERNANÇA DA INFORMAÇÃO													
1	Planejamento Estratégico da Organização												
2	Estratégia de Governança Digital												
3	Política de Segurança da Informação	**X**				**X**	**X**					**X**	
IDENTIFICAÇÃO													
1	Plano Estratégico de Identifcação de informações relevantes												
2	Equipe de Identificação												
3	Custodiantes das fontes de informações relevantes												
4	Intervalo de tempo para busca de informações relevantes							**X**					
5	Lista de palavras-chave							**X**					
6	Documentos relevantes e tipos de dados						**X**						
7	Armazenamento de dados							**X**					
8	Sistemas de e-mails												
9	Fitas de backup, equipamentos obsoletos e sistemas de Recuperação de Disastres	**X**						**X**					
10	Inventariar os sistemas legados												
11	Inventariar sistemas armazenados em nuvem ou em terceiros												
12	Verificar fontes de recursos adicionais												
13	Apresentar um relatório final com todas as fontes de ESI relevantes												

Fonte: autor, 2016.

Na análise da Tabela 4.12 destacam-se os controles 17.1.1 – Planejando a continuidade da segurança da informação; 18.1.1 – Identificação da legislação aplicável e de requisitos contratuais; 18.1.2 – Direitos de propriedade intelectual; 18.1.3 – Proteção de registros e 18.2.2 – Conformidade com as políticas e procedimentos de segurança da informação, que se relacionam com as fases de Governança da Informação e Identificação do EDRM.

No controle 17.1.1 e a sua relação com as etapas 3 da Governança da Informação e 10 da Identificação, a norma sugere respectivamente que:

- A organização determine seus requisitos para a segurança da informação e para a continuidade da gestão da segurança da informação em situações adversas, por exemplo, durante uma crise ou desastre; e
- Na ausência de um planejamento formal de continuidade do negócio e de recuperação de desastre, convém que a gestão da segurança da informação assuma que os requisitos de segurança da informação permaneçam os mesmos, em situações adversas, comparadas com as condições de operação normal. Alternativamente, uma organização pode realizar uma análise de impacto do negócio relativa aos aspectos de segurança da informação, para determinar os requisitos de segurança da informação que são aplicáveis nas situações adversas.

Uma organização que documente o planejamento quanto à continuidade da segurança da informação, pode contribuir de forma mais efetiva no processo de descoberta eletrônica. Uma política de segurança da informação e os procedimentos de continuidade de negócios podem apontar para potenciais e relevantes evidências relacionadas ao processo de *e-Discovery*.

Os controles 18.1.1, 18.1.2 e 18.1.3 são relacionados à conformidade com requisitos legais e contratuais. Uma organização que tenha formalizado processos para garantia de tais conformidades estará em melhores condições para tratar eventuais questionamentos jurídicos. Em um eventual processo de *e-Discovery*, a organização será capaz de identificar evidências de todos os esforços que envidou para cumprir a lei e os contratos assumidos.

Quanto ao controle 18.1.1 e a sua relação com a etapa 3 da Governança da Informação, a norma sugere que todos os requisitos legislativos estatutários, regulamentares e contratuais pertinentes e o enfoque da organização para atender a esses requisitos, sejam explicitamente identificados, documentados e mantidos atualizados para cada sistema de informação da organização. No controle 18.1.2 e sua relação com as etapas 3 da Governança da Informação e 6 da Identificação, a norma sugere respectivamente:

- Divulgar uma política de conformidade com os direitos de propriedade intelectual que defina o uso legal de produtos de software e de informação; e
- Manter, de forma adequada, os registros de ativos, e identificar todos os ativos com requisitos para proteger os direitos de propriedade intelectual.

No controle 18.1.3 e a sua relação com as etapas 4, 5, 7 e 9 da Identificação, a norma sugere respectivamente:

- Elaborar uma programação para retenção, identificando os registros essenciais e o período recomendado para que cada um seja mantido;
- Manter um inventário das fontes de informações-chave;
- Os procedimentos de armazenamento e manuseio sejam implementados de acordo com as recomendações dos fabricantes; e
- Cuidados sejam tomados a respeito da possibilidade de deterioração das mídias usadas no armazenamento dos registros.

Já para o controle 18.2.2, a norma sugere que os gestores identifiquem como analisar criticamente se os requisitos da segurança da informação estabelecidos nas políticas, procedimentos, normas e outras regulamentações aplicáveis, se estão sendo atendidos e as ações corretivas implementadas. Esse controle se relaciona com a etapa de Política de Segurança da Informação da fase de Governança da Informação, pois trata exatamente da questão de analisar criticamente, de forma periódica, os normativos e regulamentações que envolvem a segurança da informação.

Neste sentido, a organização que implementa os controles relacionados à análise crítica da segurança da informação contribui para o processo de descoberta eletrônica em eventuais disputas em que pode ser questionada a legalidade, os direitos relacionados à propriedade intelectual, as precauções tomadas quanto à proteção dos registros e os esforços envidados para cumprir o que determina a sua própria política de segurança da informação.

4.2. CONTRIBUIÇÕES DO E-DISCOVERY PARA A SEGURANÇA DA INFORMAÇÃO

A seção anterior apresentou a relação entre os controles da disciplina de Segurança da Informação e as fases do modelo EDRM. Foi discutido em detalhes como o processo de *e-Discovery* pode tirar proveito dos controles do SGSI que por ventura sejam implementados.

Esta seção apresenta uma perspectiva complementar em que é apontado como o SGSI pode valer-se das iniciativas de *e-Discovery* para priorizar a implementação de determinados controles, contribuindo ainda como instrumento de investigação/auditoria interna de uma organização com objetivo de aprimorar a segurança da informação.

Uma observação atenta da Tabela 4.2 demonstra que todos os 14 (catorze) controles do SGSI possuem ao menos uma relação com alguma etapa do EDRM. Entretanto, 6 (seis) controles possuem maior potencial de colaboração com o EDRM. São eles:

- A.5 Políticas de segurança da informação;
- A.6 Organização da segurança da informação;
- A.8 Gestão de ativos;
- A.12 Segurança nas operações;
- A.16 Gestão de incidentes de segurança da informação; e
- A.18 Conformidade.

Este trabalho defende o uso do *e-Discovery* como forma de aprimoramento da Segurança da Informação, tendo como ponto de partida os controles supramencionados, considerando prioritariamente as etapas indicadas na Tabela 4.2. Cada ponto de intersecção indicado na tabela traduz-se como requisitos do modelo EDRM a serem atendidos em cada um dos subcontroles.

A título de exemplo, para a implementação do controle A.8 - Gestão de Ativos, devem ser consideradas todas as informações que interessam às 12 (doze) etapas da fase de Identificação do modelo EDRM indicadas na tabela. As informações identificadas como críticas no processo de *e-Discovery* poderão ser tratadas como requisitos de implementação do controle A.8.

Ao adotar a priorização dos controles como proposto neste trabalho, uma organização pode atenuar possíveis perdas em decorrência de uma eventual ação judicial, tendo em vista que a priorização dos controles contribuiria no tratamento adequado das informações mais relevantes perante a justiça. Desta forma, a utilização preventiva do processo de *e-Discovery* apontará quais dados são mais críticos do ponto de vista jurídico, indicando os requisitos que devem ser priorizados na implementação dos controles do SGSI.

4.3. CONSIDERAÇÕES

Este capítulo apresentou as relações dos controles de segurança das normas ABNT NBR ISO 27001:2013 e 27002:2013 com as etapas e fases do modelo EDRM. As etapas do EDRM foram destacadas conjuntamente com os controles de segurança da informação à medida que a utilização de determinado controle possa favorecer a execução de uma determinada etapa do EDRM. Ressaltou-se a necessidade de atividades referente à forense digital para coleta de informações relevantes não adquiridas por meio do processo de e-Discovery, como também a importância de validar as evidências digitais perante a Justiça.

Por último, esse capítulo apresentou as contribuições do *e-Discovery* para a Segurança da Informação. O próximo capítulo apresentará as conclusões finais do trabalho e as propostas de trabalho futuro.

5. CONCLUSÃO

O processo *e-Discovery* lida com questões legais, sendo utilizado em litígios entre organizações privadas e/ou governamentais, como forma de produção de evidências eletrônicas coletadas e selecionadas de documentos digitais, e-mails, imagens, banco de dados, etc. As evidências "descobertas" podem servir como elemento de prova no processo judicial.

A principal contribuição do presente trabalho é a identificação do potencial impacto do modelo EDRM nos controles das normas ABNT NBR ISO/IEC 27001:2013 e 27002:2013. Avaliou-se o *e-Discovery* sob a perspectiva de apontar requisitos para implementação dos controles de segurança da informação. Observou-se que muitas de suas etapas apresentam características que podem contribuir para a priorização e para a implementação dos controles de um Sistema de Gestão de Segurança da Informação.

Este trabalho permitiu concluir que a organização que optar em fazer uso do processo *e-Discovery* para produção de evidências digitais, obterá vantagens e condições favoráveis se já estiver fazendo o uso dos controles de segurança da informação das normas ABNT NBR ISO/IEC 27001:2013 e 27002:2013. O contrário também é subentendido, quando os controles de segurança não existem ou estão implementados de forma precária, a organização estará suscetível a envidar um grande esforço financeiro e operacional para viabilizar o processo de *e-Discovery*, e mesmo assim sem garantias de lograr sucesso na obtenção de informações relevantes para atendimento do processo legal.

Conclui-se que o uso do modelo EDRM voltado para a descoberta digital no âmbito jurídico permite uma priorização na implementação dos controles do SGSI, minimizando assim pontos de vulnerabilidades que possam se tornar uma ameaça à segurança da informação e deixar uma organização exposta em eventuais disputas judiciais.

Outra contribuição deste trabalho foi a publicação do artigo "Processo de descobertas eletrônicas (*e-Discovery*) e seu impacto na Segurança da Informação" no Seminário de TI Inteligente na cidade de São Paulo - SP, nos dias 21 e 22 de novembro de 2016, além do artigo "*E-Discovery as a mean to Improve Information Security*", também aceito para publicação e apresentação na *Computing Conference* 2017, a ser realizada em Londres, entre os dias 18 a 20 de julho.

Em relação a trabalhos futuros, seguem algumas possibilidades:

- Avaliar como a priorização proposta dos controles de segurança da informação coincidem com os controles implementados por determinado segmento da APF;

- Quantificar a diferença de esforço para atender determinado caso de *e-Discovery*, considerando dois cenários possíveis: um que tenha os controles priorizados implementados e outro sem implementação de controles;
- Refinar o uso do processo *e-Discovery* concomitante aos controles de segurança da informação da norma ISO em contextos novos, principalmente quando externos ao ambiente de dados da instituição, como redes sociais, armazenamento em nuvem, dispositivos móveis, internet das coisas, enfim, diferentes tipos de tecnologias que estão sendo lançados constantemente;
- Avaliar como o uso da Gestão Eletrônica de Documentos – GED pode contribuir para a integridade, confiabilidade e autenticidade de documentos descobertos no processo de *e-Discovery*; e
- Relacionar conjuntamente os controles das Normas ABNT NBR ISO/IEC 27001 e 27002:2013, a legislação brasileira referente à segurança da informação e o processo de *e-Discovery*.

REFERÊNCIAS BIBLIOGRÁFICAS

ABNT NBR ISO/IEC 38500:2009. **Governança corporativa de tecnologia da informação**. ABNT - Associação Brasileira de Normas Técnicas, 2009.

ABNT NBR ISO/IEC 27001:2013. **Tecnologia da Informação – Técnicas de segurança – Sistemas de gestão da segurança da informação – Requisitos.** ABNT - Associação Brasileira de Normas Técnicas, 2013.

ABNT NBR ISO/IEC 27002:2013. **Tecnologia da Informação – Técnicas de segurança – Código de prática para controles de segurança da informação.** ABNT - Associação Brasileira de Normas Técnicas, 2013.

AKHGAR, Babak et al. **Application of Big Data for National Security**: **A Practitioner´s Guide to Emerging Technologies**. Elsevier Inc. 2015.

AULER, Pedro et al. Internacional Conference on Forensic Computer Science - ICoFCS. **Uma Nova Abordagem em Apreensão de Computadores**. 2011. Disponível em: < http://www.icofcs.org/2011/ICoFCS2011-PP18.pdf > Acesso em: Abril de 2016.

BAEZA-YATES, Ricardo; RIBEIRO-NETO, Berthier. **Recuperação de Informação-: Conceitos e Tecnologia das Máquinas de Busca.** Bookman Editora, 2013.

BASÍLIO, Susana. **A evolução dos Computadores e da Internet.** DigLitWeb: Digital Literature Web. Universidade de Coimbra, Portugal, 2006. Disponível em: < http://www.ci.uc.pt/diglit/DigLitWebCdeCodiceeComputadorEnsaio29.html > Acesso em: Dezembro de 2016.

BRANT, Des. Fernando Caldeira (Relator). **Ementa: Agravo de Instrumento – Nomeação de Perito Oficial indicado pela parte – Quebra da Imparcialidade – Impossibilidade.** Número do: 1.0382.08.096662-7/001. Tribunal de Justiça de Minas Gerais – TJMG. Publicação: 04/09/2013.

BRASIL. **Lei Complementar nº 73, de 10 de fevereiro de 1993**. Institui a Lei Orgânica da Advocacia-Geral da União e dá outras providências, 1993. Disponível em: < http://www.agu.gov.br/page/atos/detalhe/idato/177530 > Acesso em: Novembro de 2016.

BRASIL, **Lei nº 13.105, de 16 de março de 2015.** Institui o Código de Processo Civil. Disponível em : < http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2015/Lei/L13105.htm#art1046 > Acesso em: Novembro de 2016.

BRASIL. **Lei nº 9.296, de 24 de julho de 1996**. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. Brasília, 1996. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/L9296.htm > Acesso em: Novembro de 2016.

BRASIL. **Lei nº 12.735, de 30 de novembro de 2012**. Altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei no 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei no 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm > Acesso em: Novembro de 2016.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012.** Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm > Acesso em: Novembro de 2016.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm > Acesso em: Novembro de 2016.

BRASIL. **Decreto nº 8.638, de 15 de janeiro de 2016.** Institui a Política de Governança Digital no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional. Disponível em: < http://www.planalto.gov.br/CCIVIL_03/_Ato2015-2018/2016/Decreto/D8638.htm > Acesso em: Novembro de 2016.

BRASIL. **Decreto nº 8.577, de 26 de novembro de 2015.** Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da Casa Militar da Presidência da República e remaneja cargos em comissão e funções de confiança.. Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2015/Decreto/D8577.htm > Acesso em: Novembro de 2016.

BRASIL. INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO – ITI. **Sobre carimbo de tempo.** 11/08/2012. Disponível em: < http://www.iti.gov.br/component/content/article/96-perguntas-frequentes/1747-carimbo-de-tempo#oqecarimbotempo > Acesso em: Novembro de 2016.

BRASIL. SENADO FEDERAL. **Projeto de Lei nº 330/2013**. Dispõe sobre a proteção, o tratamento e o uso dos dados pessoais, e dá outras providências. Disponível em: < http://www25.senado.leg.br/web/atividade/materias/-/materia/113947 > Acesso em: Novembro de 2016.

BRASIL. SENADO FEDERAL. Agência Senado. **Projeto que protege dados pessoais passa na CCT, mas ainda vai a três comissões.** 13/10/2015
Disponível em: <http://www12.senado.leg.br/noticias/materias/2015/10/13/marco-regulatorio-para-protecao-de-dados-pessoais-e-aprovado-pela-cct-e-segue-para-tres-outras-comissoes > Acesso em: Novembro de 2016.

BRASIL. Departamento de Segurança da Informação e Comunicações do GSIPR. **Norma Complementar 20/IN01/DSIC/GSIPR (Revisão 01)**, de 15 de dezembro de 2014. Estabelece as Diretrizes de Segurança da Informação e Comunicações para Instituição do Processo de Tratamento da Informação nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. Disponível em: < http://dsic.planalto.gov.br/documentos/NC20_Revisao01.pdf >. Acesso em: Novembro de 2016.

BRASIL. **Acesso à Informação: Principais Aspectos.** Disponível em: < http://www.acessoainformacao.gov.br/assuntos/conheca-seu-direito/principais-aspectos/principais-aspectos > Acesso em: Novembro de 2016.

BRASIL. **Portal Brasileiro de Dados Abertos: O que são dados abertos?** Disponível em: < http://dados.gov.br/dados-abertos/ > Acesso em Novembro de 2016.

BRASIL. DEPARTAMENTO DE POLÍCIA FEDERAL – DPF/MJ. **Portaria nº 4453/2014-DG/DPF**, de 16 de maio de 2014. Aprova a atualização do Plano Estratégico 2010/2022, o Portfólio Estratégico e o Mapa Estratégico da Polícia Federal, e dá outras providências. 2014.

BRASIL. DEPARTAMENTO DE POLÍCIA FEDERAL – DPF/MJ. **Instrução Normativa nº 54/2012- DG/DPF**, de 12 de janeiro de 2012. Estabelece políticas e normas gerais de governança de recursos e serviços de Tecnologia da Informação no âmbito do Departamento de Polícia Federal. 2012.

BRASIL. DEPARTAMENTO DE POLÍCIA FEDERAL – DPF/MJ. **Portaria nº 779/2009-DG/DPF**, de 18 de janeiro de 2010. Institui a Política de Segurança da Informação do Departamento de Polícia Federal. 2010.

BRASIL. DEPARTAMENTO DE POLÍCIA FEDERAL – DPF/MJ. **Portaria nº 35/2010-CTI/DPF**, de 29 de julho de 2010. Dispõe sobre os critérios e procedimentos para o registro de incidentes de segurança da informação no âmbito do DPF. 2010.

BRASIL. DEPARTAMENTO DE POLÍCIA FEDERAL – DPF/MJ. **Portaria nº 01/2009-CTI/DPF**, de 14 de agosto de 2009. Implementa as atividades de Gerência de Segurança da Informação – GSI no âmbito da Coordenação de Tecnologia da Informação. 2009.

BRASIL. DEPARTAMENTO DE POLÍCIA FEDERAL – DPF. **Prestação de Contas Ordinária anual – Relatório de Gestão do Exercício de 2014. Disponível em <** http://www.pf.gov.br/acessoainformacao/relatorio_de_gestao_consolidado_2014.pdf > Acesso em: Novembro de 2016.

BRITO, Eduardo. **Segurança da Informação situa-se no Top 5 dos desafios da Governança de TI**. 2010. Disponível em: < https://goo.gl/r7YJmy > Acesso em: Novembro de 2016.

CANONGIA, Claudia; MANDARINO JUNIOR, Raphael. **Segurança cibernética: o desafio da nova Sociedade da Informação.** Parcerias Estratégicas, v. 14, n. 29, p. 21-46, 2009, ISSN 1413-9375. Disponível em: < https://goo.gl/ipJPyf > Acesso em: Novembro de 2016.

CARVALHO, Marcelo Sávio Revoredo Menezes de. **A trajetória da Internet no Brasil: do surgimento das redes de computadores à instituição dos mecanismos de governança**. DOI: 10.13140/2.1.2908.8325, Rio de Janeiro: COPPE/UFRJ, 239 p, 2006. Disponível em < https://goo.gl/5LCYwH >

CASEY, Eoghan. **Handbook of digital forensics and investigation**. Academic press, 2009.

CASEY, Eoghan. **Digital evidence and computer crime: Forensic science, computers, and the internet.** Academic press, 2011.

COSTA, Daniel Gouveia. **DNS-Um Guia para Administradores de Redes.** Brasport, 2006.

COSTA, Roberto Levi. **Metodologia e Arquitetura para Sistematização do Processo Investigatório de Análise da Informação Digital.** Dissertação de Mestrado em Engenharia Elétrica – Área de Concentração Informática Forense e Segurança da Informação. Departamento de Engenharia Elétrica – Faculdade de Tecnologia – Universidade de Brasília – UnB Brasília, 2012.

DEVAN, Ashley. The 7 V´s of Big Data. Impact Radius, 2016. Disponível em < https://www.impactradius.com/blog/7-vs-big-data/ >. Acesso em: Dezembro de 2016.

DICTIONARY.COM. **Enrom Definition**. Disponível em < http://dictionary.reference.com/browse/enron?s=t >. Acesso em: Novembro de 2016.

DICTIONARY.COM. **Instant Messaging Definition**. Disponível em < http://www.dictionary.com/browse/instant-messaging >. Acesso em: Novembro de 2016.

DICTIONARY.COM. **Patriot Act Definition**. Disponível em < http://www.dictionary.com/browse/patriot-act?s=t >. Acesso em: Novembro de 2016.

DUKE LAW. **EDRM**. Center for Judicial Studies – Durham, NC – Estados Unidos, Edição 33 de Setembro de 2016. Disponível em < https://law.duke.edu/judicialstudies/edrm/ >. Acesso em: Novembro de 2016.

EDRM, **Eletronic Discovery Reference Model Glossary**, 2016. Disponível em < http://www.edrm.net/resources/glossaries/glossary >. Acesso em: Novembro de 2016.

ERIN, M. Burke, **"Combinatorial fusion analysis: Applications for cyber security and e-discovery"**.2015. *ETD Collection for Fordham University*. Paper AAI1600741. Disponível em < http://fordham.bepress.com/dissertations/AAI1600741/ >. Acesso em: Novembro de 2016.

ESTADOS UNIDOS, Congresso. **Patriot Act.** H. R. 3162, 24 de outubro de 2001. Disponível em < https://epic.org/privacy/terrorism/hr3162.pdf >. Acesso em: Novembro de 2016.

ESTADOS UNIDOS, Department of Health and Human Services. **"HIPPA for Professionals".** Disponível em <https://www.hhs.gov/hipaa/for-professionals/index.html > Acesso em: Dezembro de 2016.

ELEUTÉRIO, Pedro M. S.; MACHADO, Márcio P. **Desvendando a Computação Forense**. 1. ed. São Paulo: Novatec, 2011.

FERREIRA, Rubens da Silva. "**A sociedade da informação como sociedade de disciplina, vigilância e controle."** Información, cultura y sociedad nº 31, Buenos Aires, p. 109 – 120, ISSN 1851-1740, 2014. Disponível em < https://goo.gl/8Wkkjo > Acesso em: Novembro de 2016.

GARRETT, Filipe. **O que é VPN? Saiba tudo sobre a rede virtual privada.** TechTudo. 01/11/2015. Disponível em < http://www.techtudo.com.br/noticias/noticia/2015/11/o-que-e-vpn-saiba-tudo-sobre-rede-virtual-privada.html > Acesso em: Novembro de 2016.

HOESCHL, Hugo Cesar. **Elementos de Direito Digital**. ISBN 85-89587-04-5, 1ª. ed. Florianópolis: Ijuris. v.1. 107p, 2003. Disponível em: < https://goo.gl/fLxu47 > Acesso em: Novembro de 2016.

HYMAN, H. S. **Learning and Relevance in Information Retrieval: A Study in the Application of Exploration and User Knowledge to Enhance Performance.** Gratuate Theses and Dissertations. Scholar Commons. University of South Florida. Janeiro de 2012. Disponível em <http://scholarcommons.usf.edu/etd/4083/>. Acesso em: Novembro de 2016.

ISACA. **COBIT 5 Portuguese**. Disponível em < http://www.isaca.org/cobit/pages/cobit-5-portuguese.aspx>. Acesso em: Novembro de 2016.

ISACA. **COBIT 5 – Modelo Corporativo para Governança e Gestão de TI da Organização.** Website: www.isaca.org**.** 2012.

ISO/IEC 27000:2016 (E). **Information technology – Security techniques – Information security management systems – Overview and vocabulary.** Internacional Standard, 2016.

KAH, Leng. T. **E-Discovery of electronically stored information in commercial litigation**, Journal of Computer Law & Security Review, v.30, nº 2, Abril de 2014, p. 171 – 178, published by Elsevier Ltd, 2014.

KERR, Orin S. **Vagueness Challenges to the Computer Fraud and Abuse Act.**, Symposium cyberspace & the law: Privacy, Property, and crime in the virtual frontier, Minnesota Law Review Foundation, vol.94, nº 5, maio de 2010. Disponível em < http://www.minnesotalawreview.org/wp-content/uploads/2012/03/Kerr_MLR.pdf >. Acesso em: Novembro de 2016.

LEDERGERBER, Marcus; KNOUFF, Matthew. **Better E-Discovery: Unified Governance and the IGRM.** American Bar Association. 11 de junho de 2012. Disponível em < http://apps.americanbar.org/litigation/committees/technology/articles/summer2012-0612-e-discovery-unified-governance-igrm.html>. Acesso em: Novembro de 2016.

LOSEY, Ralph C. **"Introduction to e-discovery: new cases, ideas, and techniques."** 532 p., American Bar Association Chicago, IL, USA, 2009.

MACIEL, Daniela. **Consumo Consciente: Redução do consumo de papel torna-se urgente - Equipamentos e softwares têm nos aproximado desse futuro**. Diário do Comércio. Belo Horizonte – MG. 27 de maio de 2015. Disponível em < http://mcfile.com/wp-content/uploads/2015/05/Diario-do-Comercio-Reportagem-eDOC-bh-2015.pdf > Acesso em: Novembro de 2016.

MIRANDA, Leví Inimá de, **Balística Forense – do Criminalista ao Legista.** 1ª ed. Rio de Janeiro: Rubio, 2014.

MIZUKOSHI, Adriano Massamithi; GARCIA, Raphael. **Cloud Computing, Um Paradigma**. ETIC- Encontro de Inciação -ISSN 21-76-8498, v. 8, n. 8, 2015.

NEWTON, Dale C.; JOHNSON, Anthony. **E-Discovery Nuts and Bolts: The Essencials of Electronic Discovery for Healthcare Professionals**. eDiscovery Healthcare Solutions, LLC, 2015.

NOGUEIRA, Michel G., **Uma visão do Anteprojeto de lei sobre o Marco Civil da Internet no Brasil com foco na Gestão da Segurança da Informação e Comunicações**. Monografia do Curso de Especialização em Gestão da Segurança da Informação e Comunicações – Universidade de Brasília. Instituto de Ciências Exatas. Departamento de Ciência da Computação, 2011.

PEREIRA, Raquel Sofia Lima. **Análise de desempenho e usabilidade em sistemas VoIP seguros**. Dissertação de Mestrado, Universidade do Minho – Escola de Engenharia, 182 p., janeiro de 2015. < http://repositorium.sdum.uminho.pt/handle/1822/35297 > Acesso em Novembro de 2016.

PINHEIRO, Patricia Peck. **Direito Digital.** 4ª ed. São Paulo: Saraiva, 2010.

PINHEIRO, Patricia Peck (organizadora). **Direito Digital Aplicado**. São Paulo: Intelligence, 2012.

PINHEIRO, Patricia Peck; HAIKAL, Victor Auilo. A nova lei de crimes digitais. Gazeta do Povo, 2013. Disponível em < http://www.gazetadopovo.com.br/vida-publica/justica-direito/artigos/a-nova-lei-de-crimes-digitais-evf935c0vqjw7rh9b4cq75tfy > Acesso em Novembro de 2016.

PHILLIPS, Amelia, et al. **E-Discovery: An Introduction to Digital Evidence**. Estados Unidos: Course Tecnology, Cengage Learning, 2013.

PLADNA, Brett. **"Computer Forensics Procedures, Tools, and Digital Evidence Bags: What they are and who should use them."** (2008). Disponível em < http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.173.7283&rep=rep1&type=pdf >. Acesso em: Novembro de 2016.

PWC. PricewaterhouseCoopers. **E-Discovery**. Disponível em < http://www.pwc.com.br/pt/forensics/ediscovery.html >. Acesso em: Novembro de 2016.

REIS, Wanderlei José dos. **"Delitos Cibernéticos: Implicações da Lei nº 12.737/12."** CONNECTION LINE 13 (2015). Disponível em < http://www.periodicos.univag.com.br/index.php/CONNECTIONLINE/article/view/251/491 > Acesso em: Novembro de 2016.

ROSS, Stephen A., et al. **Administração financeira**. AMGH Editora, 2015.

SILVA, Rafael V. R. **"Auditoria SoX e Armazenamento e Documentos_Thasco"** Fórum Contábeis – Auditoria e Perícia (2016). Disponível em < http://www.contabeis.com.br/forum/topicos/213706/auditoria-sox-e-armazenamento-de-documentosthasco/ > Acesso em: Dezembro de 2016.

TAURION, Cezar. **Big data**. Brasport, 2013.

TAKAHASHI, Tadao. **Sociedade da informação no Brasil: livro verde**. Ministério da Ciência e Tecnologia (MCT), 2000. Disponível em < https://www.governoeletronico.gov.br/documentos-e-arquivos/livroverde.pdf >. Acesso em: Novembro de 2016.

US-CERT. **Computer Forensics**. US-CERT. 2008. Disponível em < https://www.us-cert.gov/sites/default/files/publications/forensics.pdf >. Acesso em: Novembro de 2016.

WILES, Jack et al. **Techno Security's Guide to E-Discovery and Digital Forensics**: A Comprehensive Handbook. 1ª ed. Burlington, MA: Elsevier, 2007.