POLÍTICA DE INVESTIGAÇÃO FORENSE

Código: POL-TI-013
Revisão: 01
Data: 01/03/2023

WWW.DMSLOG.COM

1. INTRODUÇÃO

A DMS LOGISTICS tem a responsabilidade de garantir o cumprimento à norma ISO 27001, responsável pelas melhores práticas de segurança da informação, e à Lei Geral de Proteção de Dados Pessoais (LGPD) e seus requisitos relativos à coleta, armazenamento, recuperação e destruição de registros de dados pessoais e/ou dados sensíveis (“Dados Pessoais”).

Esta política é voltada para a investigação de incidentes que possam ocasionar em vazamento, roubo, cópia ou quaisquer ações não autorizadas nos dados e informações existentes na DMS LOGISTICS. Tal documento foi baseado no NIST.

O objetivo é estabelecer procedimentos claros sobre a investigação forense, bem como processos de identificação, coleta, aquisição e preservação das evidências digitais que possam assegurar o valor probatório das evidências e investigações, nos casos em que se mostrarem necessários.

2. GLOSSÁRIO

Aquisição da Prova Digital: Processo que envolve a criação (imagem) da Prova Digital. O resultado final deste processo é a cópia dos dados definidos.

Área de Privacidade e Proteção de Dados: Área responsável pelo suporte ao DPO (Data Protection Officer).

Ata Notarial: Comprovação escrita e com fé pública de fatos presenciados pelo notário no exercício de seu ofício.

Cadeia de Custódia: Conjunto de todos os procedimentos utilizados para manter e

documentar a história cronológica de evidência, para rastrear sua posse e manuseio a partir de seu reconhecimento até o seu descarte, garantindo, assim, a preservação do valor probatório.

Carimbo do Tempo: Parâmetro de variação de tempo que indica o momento específico que diz respeito a uma referência de tempo comum.

Cartões SIM (SubscriberIdentity Module, Módulo de identificação de Assinante) e USIM: Universal SubscriberIdentity Module, Módulo Universal de Identificação de Assinante). Cartões quesão usados para comunicação, sendo o primeiro para comunicação em redes GSM e o segundo para redes UMTS (3G).

Coleta de Prova Digital: Processo de recolhimento de itens físicos que contêm potencial Prova Digital.

Confiabilidade da Prova Digital: Garantia que a Prova Digital é passível de auditoria e repetibilidade por outras autoridades e colaboradores.

Dados Voláteis: Dados que são propensos a alteração e podem ser facilmente modificados ou perdidos.

Especialista em Evidência Digital (DES): Colaborador autorizado, treinado e qualificado para manusear a evidência digital.

Dispositivo Digital: Equipamento ou recurso utilizado para processar ou armazenar dados digitais.

Especialista em Evidência Digital (DES): Colaborador autorizado, treinado e qualificado para manusear a evidência digital.

Evidência Digital: Dados armazenados ou transmitidos na forma digital, que poderão ser utilizados como evidência.

Função de Verificação / Hash: Função usada para verificar dois conjuntos de dados idênticos.

Identificação da Prova Digital: Processo de busca, reconhecimento e documentação da Prova Digital.

Mouse-Jugglers: Recurso utilizado para evitar que o dispositivo entre em modo de espera.

Preservação da Prova Digital: Processo para manter e proteger a integridade e/ou a condição original da Prova Digital.

Processo de Aquisição da Prova Digital: Processo em que é realizada a duplicação da Prova Digital para outro dispositivo no próprio ambiente físico.

Processo de Coleta da Prova Digital: Processo em que o dispositivo que armazena potenciais evidências digitais é removido do ambiente original e levado para que seja realizada a cópia em outra área da organização.

Relevância da Prova Digital: Garantia que a evidência digital é relevante para a investigação do incidente.

Suficiência da Prova Digital: Garantia que a Prova Digital coletada ou adquirida é suficiente para permitir a sua utilização adequada.

Tentativa de Burla: Tentativa de burlar as diretrizes e controles estabelecidos, quando constatada, deve ser tratada como uma violação.

Violação: Qualquer atividade que desrespeite as regras estabelecidas nesta Política e em documentos complementares.

3. INVESTIGAÇÃO FORENSE

A análise forense de computadores e redes evoluiu para garantir a apresentação adequada de dados probatórios de crimes cibernéticos. Ferramentas forenses e técnicas são pensadas no contexto de investigações criminais, segurança de equipamentos e tratamento de incidentes - usado para responder a um evento investigando sistemas suspeitos, coletando e preservando evidências, reconstruindo eventos e avaliando o estado atual de um evento. No entanto, ferramentas e técnicas forenses também são úteis para muitos outros tipos de tarefas, como as seguintes:

Solução de problemas operacionais. Muitas ferramentas e técnicas forenses podem ser aplicadas para solucionar problemas operacionais, como encontrar a localização virtual e física de um host com uma configuração de rede incorreta, resolvendo um problema funcional com um aplicativo e gravando e revisando as configurações atuais do sistema

operacional e do aplicativo para um host.

Monitoramento de registros. Várias ferramentas e técnicas podem auxiliar no monitoramento de logs, como analisar entradas de log correlacionadas em vários sistemas. Isso pode ajudar nos incidentes de manipulação, identificação de violações de políticas, auditoria e outros esforços.

Recuperação de dados. Existem dezenas de ferramentas que podem recuperar dados perdidos de sistemas, incluindo dados que foram acidentalmente ou propositadamente excluídos ou modificados. A quantidade de dados que podem ser recuperados varia de caso a caso.

Aquisição de dados. Algumas organizações usam ferramentas forenses para adquirir dados de hosts que estão sendo reimplantados ou aposentados. Por exemplo, quando um usuário sai de uma organização, os dados da estação de trabalho do usuário podem ser adquiridos e armazenados caso seja necessário no futuro. A estação de trabalho pode então ser higienizada para remover todos os dados do usuário original.

DueDiligence/Conformidade Regulamentar. As regulamentações existentes e emergentes exigem muitas organizações para proteger informações confidenciais e manter determinados registros para fins de auditoria.

Além disso, quando informações protegidas são expostas a outras partes, as organizações podem ser obrigadas a notificar outras agências ou indivíduos afetados. A perícia pode ajudar as organizações a exercerem o devido diligência e cumprir tais requisitos.

Independentemente da situação, o processo forense compreende as seguintes fases básicas:

1. **Coleção**. A primeira fase do processo é identificar, rotular, registrar e adquirir dados das possíveis fontes de dados relevantes, seguindo as diretrizes e procedimentos que preservam a integridade dos dados. A coleta é normalmente realizada em tempo hábil devido à probabilidade de perder dados dinâmicos, como conexões de rede atuais, bem como perder dados de dispositivos alimentados por bateria (por exemplo, tablets, telefones celulares).
2. **Exame.** Os exames envolvem o processamento forense de grandes quantidades de dados coletados usando uma combinação de métodos automatizados e manuais para avaliar e

extrair dados de interesse, preservando a integridade dos dados.

3. **Análise.** A próxima fase do processo é analisar os resultados do exame, utilizando métodos e técnicas justificáveis, para obter informações úteis que abordem as questões que foram o impulso para a realização da coleta e do exame.

4**. Comunicando.** A fase final é relatar os resultados da análise, que pode incluir a descrição das ações utilizadas, explicando como as ferramentas e procedimentos foram selecionados, determinando quais outras ações precisam ser executadas (por exemplo, exame forense de fontes de dados adicionais, segurança, vulnerabilidades identificadas, melhoria dos controles de segurança existentes) e fornecendo recomendações para melhoria de políticas, diretrizes, procedimentos, ferramentas e outros aspectos da perícia forense processo. A formalidade da etapa de notificação varia muito dependendo da situação.

5. **Lições aprendidas.** Após a investigação, deverá ser feita uma reunião com a Alta Administração da DMS LOGISTICS., o CISO, o Gestor de Segurança da Informação e a Equipe de Segurança da Informação para avaliar os resultados e discutir pontos de melhoria.

4. PAPÉIS E RESPONSABILIDADES

Equipe Forense

Para realizar investigações e análises forenses de computadores e redes, é preciso ter a determinação de papéis e responsabilidades dos profissionais envolvidos. Embora exista a possibilidade de adesão de outros profissionais, de acordo com o cenário concreto, todos os processos de investigação e coleta de provas digitais envolverão os grupos a seguir:
CISO: É o responsável pela estratégia da análise forense, especifica a forma de coleta de evidências e aprova os documentos, relatórios e evidências coletadas.

Gestor de Segurança da Informação: É o responsável por verificar se as diretrizes passadas pelo CISO estão sendo cumpridas. Converte as estratégias em ações táticas e acompanha a Equipe de Investigadores nos trabalhos.

Encarregado de Dados: Caso a investigação envolva dados pessoais, seja de colaboradores ou terceiros, o Encarregado de Dados deverá supervisionar os documentos, relatórios e acompanhar a adoção de medidas técnicas protetivas para assegurar a confidencialidade dos dados, a comunicação com os Titulares e a Autoridade Nacional de Proteção de Dados

e outros interessados, de acordo com a situação concreta.

Investigador líder: É responsável pela análise forense, garantindo que os procedimentos sejam seguidos para manter a integridade das informações.

Equipe de investigadores: São os membros, em nível operacional, que investigam os casos com indícios de violações, sejam elas criminosas (intencionais) ou acidentais.

Utilizam muitas técnicas e ferramentas forenses. É composta por outros investigadores e pode incluir consultores jurídicos, membros do departamento de Recursos Humanos, Departamento Financeiro, e do Encarregado de Dados (DPO) em caso de comprometimento de dados pessoais. Os agentes responsáveis pela aplicação da lei e outros fora da organização que possam realizar investigações criminais não são considerados parte do grupo interno de uma organização de investigadores.

Profissionais de Tecnologia da Informação (TI) e Segurança da Informação (SI): Este grupo inclui a equipe de suporte técnico e sistema, rede e segurança, bem como, em caso de necessidade, dos seus administradores. Eles usam um pequeno número de técnicas forenses e ferramentas específicas para sua área de atuação, experiência durante seu trabalho de rotina (por exemplo, monitoramento, solução de problemas, recuperação de dados).

Agentes Externos: Caso a situação concreta exija analistas especializados em determinada área de atuação, eles podem ser chamados para realizar perícias forenses, como o envio de mídia

fisicamente danificada para um empresa de recuperação de dados para reconstrução, ou ter pessoal de aplicação da lei especialmente treinado ou os consultores coletam dados de uma fonte incomum (por exemplo, telefone celular). Se, no processo de investigação, for necessário o uso de software especializado, equipamentos, instalações e conhecimentos técnicos que excedam o conhecimento da Equipe de Investigadores, poderão ser chamados agentes externos para realizar tarefas específicas.

A Equipe Forense, em especial o Investigador líder, a Equipe de investigadores e os Profissionais de Tecnologia da Informação (TI) e Segurança da Informação (SI) têm as seguintes responsabilidades:

1. Garantir a auditabilidade, repetibilidade, reprodutibilidade e justificabilidade da evidência digital;

2. Examinar o ambiente físico e lógico e identificar fontes de dados internas e externas;

3. Priorizar as fontes e estabelecer a ordem que os dispositivos ou dados devem ser coletados ou adquiridos;

4. Autorizar ou não a presença de colaboradores no ambiente físico do incidente, quando a necessidade de manuseio de evidência for originada por incidente;

5. Garantir a integridade dos dispositivos durante o processo de análise do ambiente físico;
6. Determinar qual colaborador é responsável pelo ambiente físico;
7. Documentar o ambiente e todos os dispositivos;

8. Garantir, sempre que necessário, a autorização ou presença do responsável pelo material ou dispositivo;

9. Analisar a potencial evidência digital, nos termos desta Política;

10. Portar os recursos necessários para o processo de coleta e aquisição da evidência digital;

11. Solicitar, sempre que necessário suporte técnico ou jurídico;

12. Decidir sobre a coleta ou aquisição de uma evidência digital;

13. Coletar as evidências digitais em dispositivos ligados, desligados ou em rede, nos termos desta Política;

14. Adquirir as evidências digitais em dispositivos ligados, desligados ou em rede, nos termos desta Política;

15. Analisar quanto à necessidade de aquisição parcial de evidências digitais, nos termos desta Política;

16. Realizar a aquisição imediata de dispositivos digitais de missão crítica, nos termos desta Política;

17. Realizar a coleta ou aquisição de mídia de armazenamento digital removível; 18. Realizar a preservação da evidência digital em local seguro e com acesso restrito; 19. Realizar o registro da cadeia de custódia da evidência digital;

20. Transportar a evidência digital de modo seguro;

21. Documentar todo o processo de identificação, coleta, aquisição, transporte e preservação da evidência digital;

22. Manter a confidencialidade de todo o processo de manuseio e conteúdo da evidência digital.

5. DIRETRIZES GERAIS

O manuseio adequado de uma evidência digital é essencial para garantir a sua auditabilidade, repetibilidade, reprodutibilidade e justificabilidade, o que contribuirá para a admissibilidade da evidência digital em processos judiciais, administrativos ou disciplinares.

A evidência digital pode se originar de diferentes tipos de dispositivos e ambientes digitais, como redes, bancos de dados, Internet, discos rígidos, dispositivos móveis e até sistemas.

Para garantir a confiabilidade da evidência digital, os procedimentos de identificação, coleta, aquisição e preservação devem contar com:

1. Aplicação dos procedimentos descritos neste documento;

2. Documentação de todas as ações realizadas;

3. Indicação de DES qualificado durante o processo de manuseio da evidência digital. O manuseio da evidência digital deve ser realizado de acordo com as leis e regulamentações nacionais. Além disso, o DES deve considerar a sua relevância, confiabilidade e suficiência para a DMS LOGISTICS.

Se for identificado um incidente/violação que ocasione vazamento de dados pessoais, o Encarregado de Dados (DPO), a equipe de Privacidade e os responsáveis pela Segurança da Informação e Resposta a Incidentes devem ser imediatamente acionados e iniciar o plano de contenção, preservação, recuperação e investigação sobre o ocorrido.

Os demais passos seguirão os procedimentos a seguir.

6. PROCEDIMENTOS OPERACIONAIS PRÉVIOS

Caso uma atividade suspeita seja identificada, ela deve ser imediatamente reportada ao Gestor de Segurança da Informação e ao CISO. O Gestor de Segurança da Informação verificará se o caso exige uma investigação forense. Caso entenda necessário, enviará um comunicado por e-mail ao CISO, solicitando a abertura de investigação. O Gestor de Segurança da Informação determinará, de acordo com a situação concreta, a coleta do equipamento potencialmente envolvido na situação e o manterá em local seguro.

Se o CISO aprovar a investigação, ele dará as orientações fará a convocação da Equipe Forense. A investigação será considerada iniciada a partir dessa convocação.

A Equipe Forense deverá fazer uma análise prévia para verificar se é necessário prosseguir com a investigação ou se se trata de um falso alerta.

Decidido o prosseguimento da investigação, a Equipe Forense estabelecerá um cronograma das ações e determinará quais métodos, ferramentas, dispositivos e sistemas serão investigados. A partir daí, é criada a cadeia de custódia, melhor descrita em tópico especificado em outra seção deste documento.

Todas as evidências serão armazenadas em local específico, designado na abertura da investigação.

Será mantido um inventário com todas as evidências coletadas, sob responsabilidade da equipe de Segurança da Informação e do Gestor de Segurança da Informação.

Passa-se, então, às fases de coleta, análise, relatório e lições aprendidas, descritos a seguir.

7. TEMPO DE RESPOSTA

O processo de investigação forense deve ser iniciado no prazo máximo de 24 horas a partir do conhecimento da violação.

8. SENSIBILIDADE OS DADOS

Se for observada a existência de dados pessoais, sejam sensíveis ou não, ou outras questões

que envolvam privacidade, sensibilidade de informações e segredos comerciais ou industriais, poderão existir restrições para a participação de agentes externos na investigação.

Nestes casos, será preferível manter esses dados, informações, equipamentos ou sistemas sob seu próprio controle para proteger a privacidade dos dados.

Princípios norteadores da Investigação Forense

Durante o manuseio da evidência digital, o Investigador Líder, a Equipe de Investigadores e o DES devem garantir:

1. **Auditabilidade:** garantia que as atividades realizadas durante o procedimento de coleta ou aquisição possam ser avaliadas (auditadas) por um terceiro autorizado;

2. **Repetibilidade:** garantia que o procedimento de coleta ou aquisição possa ser repetido, sob as mesmas condições e ferramentas, de forma a alcançar o mesmo resultado. Caso as condições não permitam a repetibilidade do teste, por exemplo, em caso de memória volátil, esse fato deve estar documentado na cadeia de custódia;

3. **Reprodutibilidade:** garantia que, quando em condições e ferramentas diferentes, o resultado obtido pela coleta ou aquisição da evidência digital possa ser reproduzido;

4**. Justificabilidade:** garantia que o responsável pela coleta ou aquisição seja capaz de justificar todas as ações e os métodos utilizados para o tratamento da evidência digital.

9. INVESTIGAÇÃO FORENSE

O objetivo, ao realizar uma perícia forense, é obter uma melhor compreensão de um evento de interesse para encontrar e analisar os fatos relacionados a esse evento.

Ela pode ser necessária em muitas situações diferentes, como coleta de provas para processos judiciais, ações disciplinares, tratamento de incidentes de malware e problemas

operacionais incomuns. A perícia deve ser realizada usando o processo de quatro fases: coleta, exame, análise e relatório com conclusões, que serão abordadas durante a política.

Esta seção descreve as fases básicas do processo forense: coleta, exame, análise e comunicando.

A investigação deverá ser guiada pelos seguintes questionamentos:

1. Qual o objetivo/finalidade da investigação?

2. Qual o foco da investigação?

3. Quais as questões serão investigadas?

4. Quais respostas poderão ser conseguidas com a investigação?

5. Quais os dados relevantes para obter essas respostas?

Durante a coleta, os dados relacionados a um evento específico são identificados, rotulados, registrados e coletados, e sua integridade é preservada.

Na segunda fase, é feito o exame, com o uso de ferramentas e técnicas forenses apropriados aos tipos de dados que foram coletados para identificar e extrair as informações dos dados coletados, protegendo sua integridade. O exame pode usar uma combinação de ferramentas automatizadas e processos manuais.

A próxima fase, análise, envolve a análise dos resultados do exame para obter informações úteis que abordam as questões que foram o ímpeto para realizar a coleta e exame.

A fase final envolve relatar os resultados da análise, que pode incluir a descrição das ações executadas, determinando quais outras ações precisam ser executadas e recomendando melhorias nas políticas, diretrizes, procedimentos, ferramentas e outros aspectos do processo forense.

10. MANUSEIO DA PROVA DIGITAL

A prova digital pode ser alterada, alterada ou destruída por manuseio impróprio, tornando-a inutilizável. Por isso, é essencial que:

1. O dispositivo ou dado original, assim como o material coletado ou adquirido, sejam

manuseados o mínimo possível e somente pelas pessoas designadas;

2. Todas as ações realizadas sejam documentadas;

3. Sejam identificadas e registradas todas as pessoas que tiveram acesso à evidência digital e ao local.

11. IDENTIFICAÇÃO DA PROVA DIGITAL

A evidência digital pode ser representada de forma:

1. Física, por exemplo: o computador de mesa ou dispositivos móveis;

2. Lógica, por exemplo: os dados ou aplicações em um dispositivo.

Para identificar uma evidência digital, o responsável designado (Investigador Líder/DES) deve tomar conhecimento do incidente, realizar o reconhecimento do ambiente físico e lógico e das possíveis fontes de dados, sejam elas internas ou externas.

É essencial que, antes de iniciar o procedimento de identificação da evidência digital, o Investigador Líder/DES tenha detalhes sobre o incidente que demandou a sua atividade.

Assim, ao examinar o ambiente físico e lógico onde será coletada ou adquirida a evidência digital, o Investigador Líder/DES deve identificar fontes internas de dados, como:

1. Computadores desktops;

2. Servidores;

3. Dispositivos de armazenamento em rede;

4. Notebooks, celulares, smartphones e tablets;

5. Pen drives, CDs, DVDs e portas USB;

6. Cartões de memória flash;

7. Impressoras;

8. Mídias de Backup;

9. Sistemas.

Também podem ser identificadas fontes externas de dados, como:

1. Atividades realizadas via Web;

2. Computação em nuvem;

3. Dispositivos pessoais ou de terceiros.

A identificação deve priorizar as fontes e estabelecer a ordem que os dispositivos serão coletados ou os dados adquiridos, considerando:

1. Valor dos dados;

2. Volatilidade dos dados;

3. Quantidade de esforços necessários (tempo gasto, custo de equipamentos e serviços).

Nesta etapa, o Investigador Líder/DES deve garantir que os dispositivos permaneçam no estado que se encontram, ou seja, se estiverem ligados, permanecerão ligados; se estiverem desligados, permanecerão desligados.

O Investigador Líder/DES deve avaliar se os dispositivos que utilizam bateria precisam ser carregados na fonte de energia para assegurar que dados não sejam perdidos.

12. ANÁLISE DO AMBIENTE FÍSICO DO INCIDENTE

O ambiente físico da evidência digital deve ser preservado e acessado somente pelo Investigador Líder/DES e pelos colaboradores por ele autorizados.

Antes de iniciar a coleta ou aquisição da evidência digital, o Investigador Líder/DES deve:

1. Assegurar e assumir o controle do ambiente físico onde os dispositivos estão;

2. Determinar qual colaborador será responsável pelo ambiente físico;

3. Garantir que os colaboradores estejam afastados dos dispositivos e fontes de energia;

4. Documentar qualquer colaborador que tenha acesso ao ambiente ou possa estar envolvido com o incidente/;

5. Documentar a cena e todos os seus dispositivos (fotografar ou realizar anotações);

6. Pesquisar itens como notas, rascunhos, agendas, papéis, anotações e dispositivos móveis no ambiente;

7. Desativar as conexões bluetooth e redes sem fio dos dispositivos móveis dos colaboradores;

8. Utilizar, caso seja necessário, detector de sinais de rede sem fio.

13. PRESENÇA DOS RESPONSÁVEIS

Caso a evidência digital coletada ou adquirida não seja de propriedade da DMS LOGISTICS., o Investigador Líder/DES deve assegurar que possui autorização e esteja presente o responsável pelo dispositivo.

14. ANÁLISE DO POTENCIAL PROVA DIGITAL

Para análise de potencial evidência digital, o Investigador Líder/DES deve considerar os seguintes aspectos antes de iniciar qualquer atividade:

1. Qual método de coleta ou aquisição será aplicado no caso;

2. Qual é o nível de volatilidade dos dados relacionados à potencial evidência digital; 3. Quais recursos serão necessários;

4. Se é possível identificar a existência de alguma conexão remota ao dispositivo e se isso oferece alguma ameaça à integridade de potencial evidência digital;

5. O que fazer caso o dispositivo ou dado esteja danificado ou comprometido;

6. O que fazer caso algum dispositivo esteja configurado para destruir ou ofuscar um dado se desligado ou acessado de forma descontrolada.

Além disso, o Investigador Líder/DES deve considerar as seguintes circunstâncias:

1. Se existe permissão legal ou autorização formal do responsável do dispositivo para realizar a sua coleta caso o dispositivo não seja de propriedade da DMS LOGISTICS.;

2. Se existe a necessidade da lavratura de ata notarial, a fim de autenticar e comprovar a verdade de fatos ou estado dos dados;

3. Se existe a necessidade de utilizar outro método para aquisição da evidência;

4. Obrigatoriedade da aquisição ou coleta ocorrer em sigilo. Sempre que possível esta atividade deve ocorrer em horários e dias que possuam a menor concentração de pessoas;

5. Se o dispositivo for de missão crítica, qual é o período de tolerância para realizar qualquer atividade.

Para o processo de coleta ou aquisição da evidência digital, o Investigador Líder/DES deve

portar os seguintes recursos:

1. Estação de trabalho forense;

2. Dispositivos para armazenamento de dados;

3. Mídias em branco;

4. Material para manipulação e registro das evidências, por exemplo, sacos lacrados para armazenamento das evidências, bloco de anotações, etiquetas e câmeras fotográficas;

5. Proteção física do ambiente físico, se necessário.

O Investigador Líder/DES deve solicitar suporte técnico ou jurídico, sempre que necessário, junto às demais áreas da DMS LOGISTICS ou de empresas terceirizadas.

Para adquirir ou coletar dados de fontes externas ou de modo intrusivo, o Investigador Líder/ DES deve contatar e envolver o Departamento Jurídico, pois pode depender de ações judiciais, extrajudiciais, cláusulas contratuais ou normativos internos.

15. PROCESSO DE DECISÃO: COLETAR OU ADQUIRIR PROVA DIGITAL

Para o Investigador Líder/DES decidir sobre a coleta ou aquisição de uma evidência digital, deve observar:

1. Volatilidade dos dados;

2. Permissão legal ou autorização para realizar a coleta do dispositivo ou aquisição da evidência, caso não seja da DMS LOGISTICS;

3. Confidencialidade da coleta ou aquisição;

4. Criticidade do sistema ou do dispositivo;

5. Existência de criptografia completa de disco, ou de volumes nos quais as chaves e senhas possam residir como dado volátil;

6. Recursos, como tamanho do outro dispositivo para aquisição da evidência ou

disponibilidade (tempo) do DES;

7. Necessidade de manutenção ou restabelecimento da atividade ou serviço da DMS LOGISTICS.

Segue abaixo fluxo para tomada de decisão em coletar ou adquirir uma evidência digital:

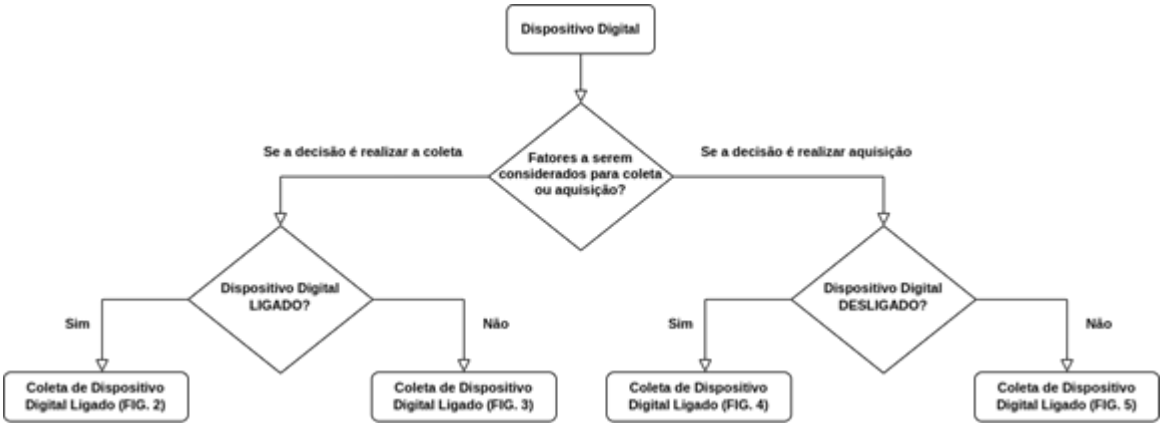


Figura 1 - Fluxo para tomada de decisão. Fonte: ABNT NBR ISO/IEC 27037:2013
Após definir pela coleta ou aquisição da evidência digital, o Investigador Líder/DES deve formalizar o que motivou sua decisão e definir quando a ação será realizada.

Caso avalie que determinada evidência digital não deve ser coletada ou adquirida, sua decisão também deve ser documentada e justificada.

16. COLETA DE DADOS: DISPOSITIVOS LIGADOS

O primeiro passo no processo de investigação forense é identificar fontes potenciais de dados e adquirir dados delas. Nessa fase, os dados são identificados, coletados e inventariados. Os investigadores devem pensar em possíveis fontes de dados localizadas em outros lugares, além da variedade de fontes de dados disponíveis.

A Equipe Forense coletou dados relevantes dos dispositivos e sistemas sob suspeita de violação. O objetivo é fornecer uma análise detalhada das informações encontradas. Os dados serão identificados, rotulados, registrados e coletados.

Caso seja necessário, o dispositivo ou sistema poderão ser isolados, desligados ou outros procedimentos específicos à situação.

Caso a Equipe Forense identifique essa necessidade, os e-mails corporativos poderão ser objeto de coleta e investigação de evidências. Neste caso, os e-mails deverão ser exportados e salvos no local de armazenamento designado para o caso em análise. Deverão ser identificados: quem exportou os e-mails, como e quando isso foi feito e onde as mensagens foram transferidas e armazenadas. Essas informações serão documentadas, de forma a serem consultadas e rastreadas, se necessário.

Além disso, a equipe responsável pela investigação deverá discutir as considerações de resposta a incidentes, enfatizando a necessidade de calcular o valor dos dados coletados, em relação aos custos e impacto para a organização da coleta do processo.

Para o processo de coleta de evidência digital em dispositivos ligados, o Investigador Líder/DES deve considerar:

1. Aquisição de dados voláteis, antes de desligar o sistema ou remover a fonte de energia;

2. Verificar a existência de chaves de criptografia e outros dados cruciais na memória ativa ou inativa;

3. Verificar a possibilidade de realizar a aquisição da evidência quando há suspeita do uso de criptografia, com o uso de fontes de alimentação portáteis para não interromper a energia do dispositivo ou mouse-jugglers para impossibilitar a ativação do protetor de tela;

4. Verificar a confiabilidade ou não do sistema;

5. Verificar a configuração do dispositivo, a fim de determinar se será desligado por meio de procedimentos normais ou removido da fonte de energia. Caso a decisão seja por remover da fonte de energia, o Investigador/DES deve retirar primeiro a extremidade do cabo ligada ao dispositivo;

6. Acondicionar o dispositivo cuidadosamente e etiquetar;

7. Estabelecer a cadeia de custódia.

Abaixo segue o fluxo para coleta de evidência digital em dispositivos ligados:

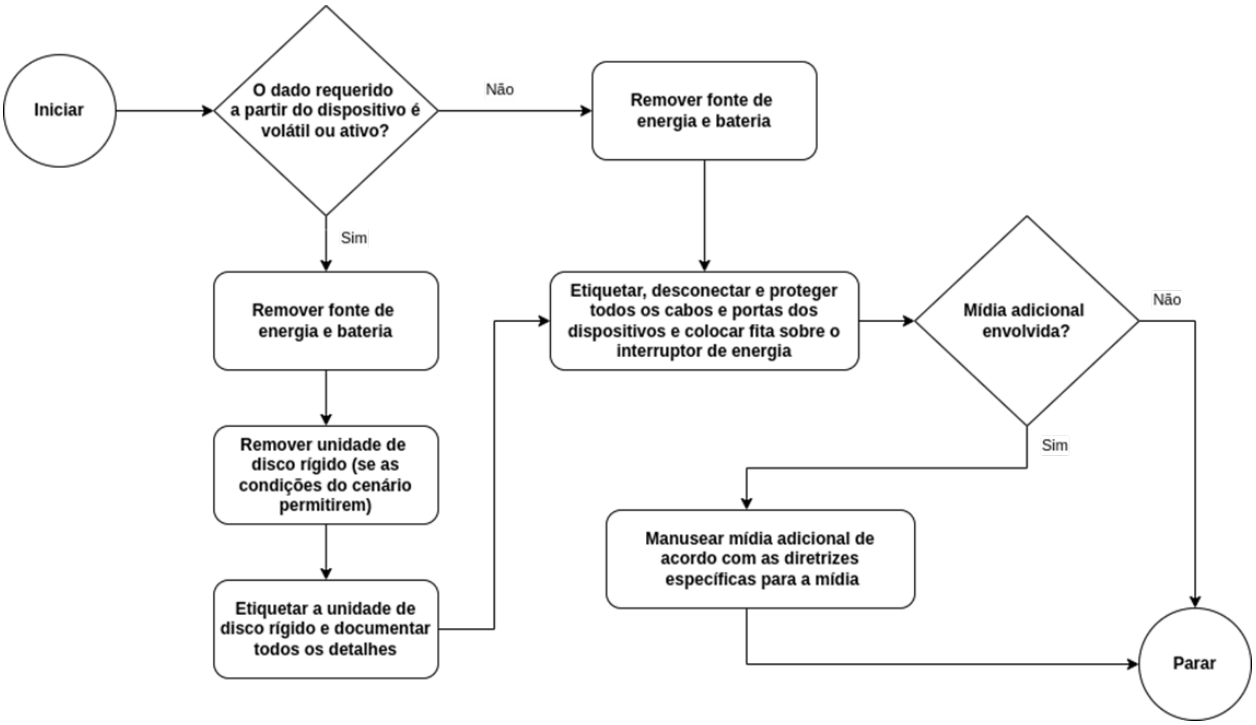


Figura 2 - Coleta de evidência digital em dispositivos ligados. Fonte: ABNT NBR ISO/IEC 27037:2013

17. COLETA: DISPOSITIVOS DESLIGADOS

Antes de iniciar o processo de coleta de dispositivos desligados, o Investigador/DES deve se

certificar que estão efetivamente desligados, e não em modo de espera.

Para o processo de coleta de evidência digital em dispositivos desligados, o Investigador/DES deve:

1. Remover a fonte de energia, retirando, primeiramente, a extremidade ligada ao dispositivo; 2. Certificar-se que as bandejas de CD e DVD estejam vazias e retraídas de modo adequado; 3. Desconectar e proteger todos os cabos do dispositivo e etiquetar as portas de conexão; 4. Colocar fita sobre o interruptor de energia, se necessário;

5. Acondicionar o dispositivo cuidadosamente e etiquetar;

6. Estabelecer a cadeia de custódia.

As mídias adicionais envolvidas devem ser removidas do dispositivo e manuseadas como evidência complementar. É importante identificar em qual porta a mídia está conectada no dispositivo.

Abaixo segue o fluxo para coleta de evidência digital em dispositivos desligados:

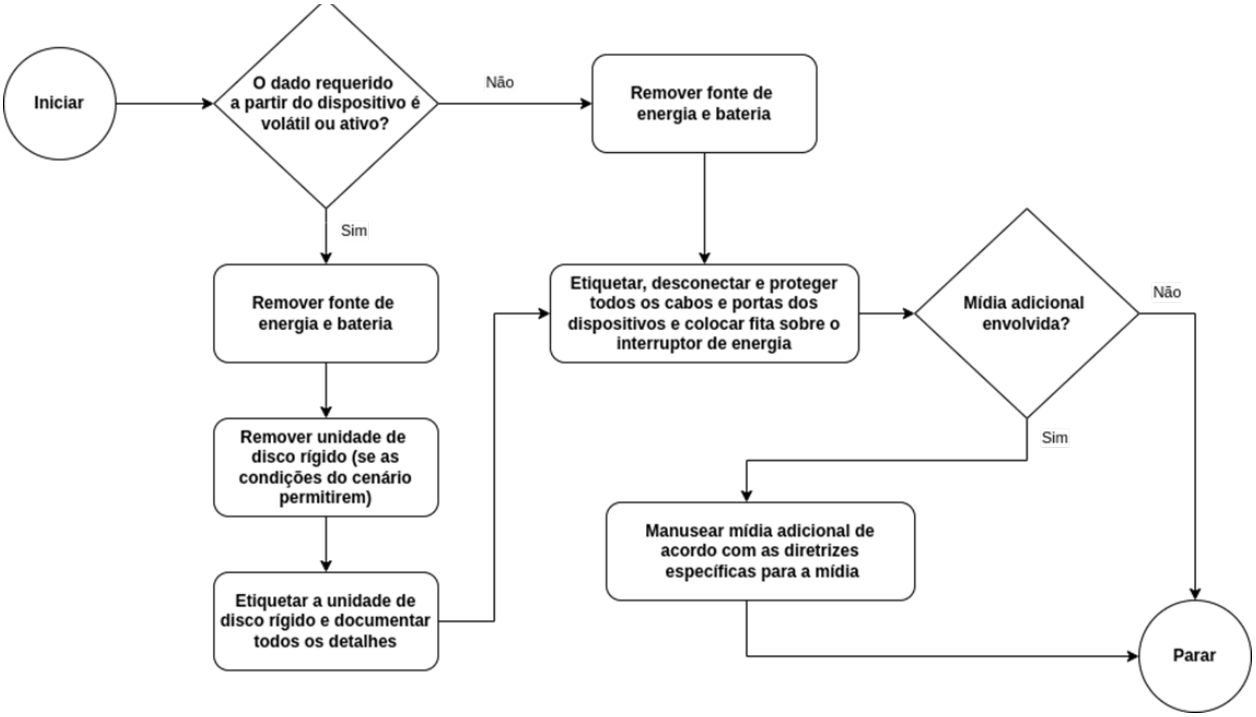


Figura 3 - Coleta de evidência digital em dispositivos desligados. Fonte: ABNT NBR ISO/IEC 27037:2013

18. COLETA: DISPOSITIVOS EM REDE

Para o processo de coleta de dispositivos em rede, o Investigador/DES deve:

1. Desconectar o dispositivo somente após certificar-se que nenhuma evidência digital será perdida, conforme volatilidade dos dados;

2. Identificar os serviços de comunicação, como rede sem fio ou bluetooth, a fim de proteger a evidência digital contra destruição;

3. Antes de desconectar o dispositivo de redes com fio, traçar as conexões até os dispositivos e identificar as portas para futura reconstrução da rede;

4. Verificar se é necessário conectá-lo a uma fonte de energia;

5. Verificar se é necessário desligar o dispositivo no momento da coleta para prevenir que o dado seja alterado;

6. Se o dispositivo estiver desligado, mantenha desligado;

7. Acondicionar o dispositivo cuidadosamente e etiquetar;

8. Estabelecer a cadeia de custódia.

19. EXAME DOS DADOS

Após a coleta de dados, a próxima fase é examinar os dados, que envolvem avaliar e extrair as informações relevantes dos dados coletados. Ela buscará responder às perguntas surgidas pela suspeita de violação.

Esta fase também pode envolver contornar ou mitigar os recursos do sistema operacional ou do aplicativo que obscurecem dados e códigos, como compactação de dados, criptografia e mecanismos de controle de acesso. Um disco rígido adquirido pode conter centenas de milhares de arquivos de dados; identificar os arquivos de dados que contêm informações de interesse, incluindo informações ocultadas por meio de compactação de arquivos e controle de acesso. Além disso, arquivos de dados de interesse podem conter informações estranhas que devem ser filtradas, ou seja, apenas

as informações relacionadas ao evento sob investigação devem ser analisadas.

A Equipe Forense poderá usar diversas ferramentas e técnicas para investigar, interpretar, filtrar e reduzir a quantidade de dados que precisam ser peneirados. As pesquisas de texto e padrão podem ser usadas para identificar dados pertinentes, como encontrar documentos que mencionam um assunto ou pessoa em particular, ou identificar entradas de log de e-mail para um endereço de e-mail específico. Outra técnica que pode ser usada é usar uma ferramenta que possa determinar o tipo de conteúdo de cada arquivo de dados, como texto, gráficos, música ou um arquivo compactado. O conhecimento dos tipos de arquivos de dados pode ser usado para identificar arquivos que mereçam um estudo mais aprofundado, bem como excluir arquivos que não interessam ao exame. O mesmo pode ser aplicado aos bancos de dados contendo informações sobre arquivos conhecidos, que também podem ser usados para incluir ou excluir arquivos de uma consideração mais aprofundada.

A Equipe deverá fazer um cronograma detalhado dos eventos, com análise dos dispositivos e sistemas e elaborar um relatório, que será encaminhado ao CISO.

20. AQUISIÇÃO DE PROVA DIGITAL

O procedimento de aquisição de evidência digital deve utilizar ferramentas validadas e confiáveis, de modo a evitar efeitos indesejados ou não previstos sobre o sistema.

O DES deve definir, de acordo com a criticidade, se há necessidade de lavrar Ata Notarial do processo da aquisição de evidência digital (por exemplo, do processo que gerou a cópia idêntica dos dados) ou da evidência adquirida (como página da Internet, publicação em um site).

A aquisição da evidência digital deve gerar uma duplicação bit-a-bit dos dados ou dispositivos originais. A fonte original e a cópia da evidência digital devem produzir o mesmo resultado de função de verificação (hash).

O DES deve, preferencialmente, realizar uma duplicação bit-a-bit do que está no dispositivo digital. Caso não seja possível, podem ser realizadas cópias de dados específicos.

Para o processo de aquisição de evidência digital em dispositivos ligados, o DES deve considerar:

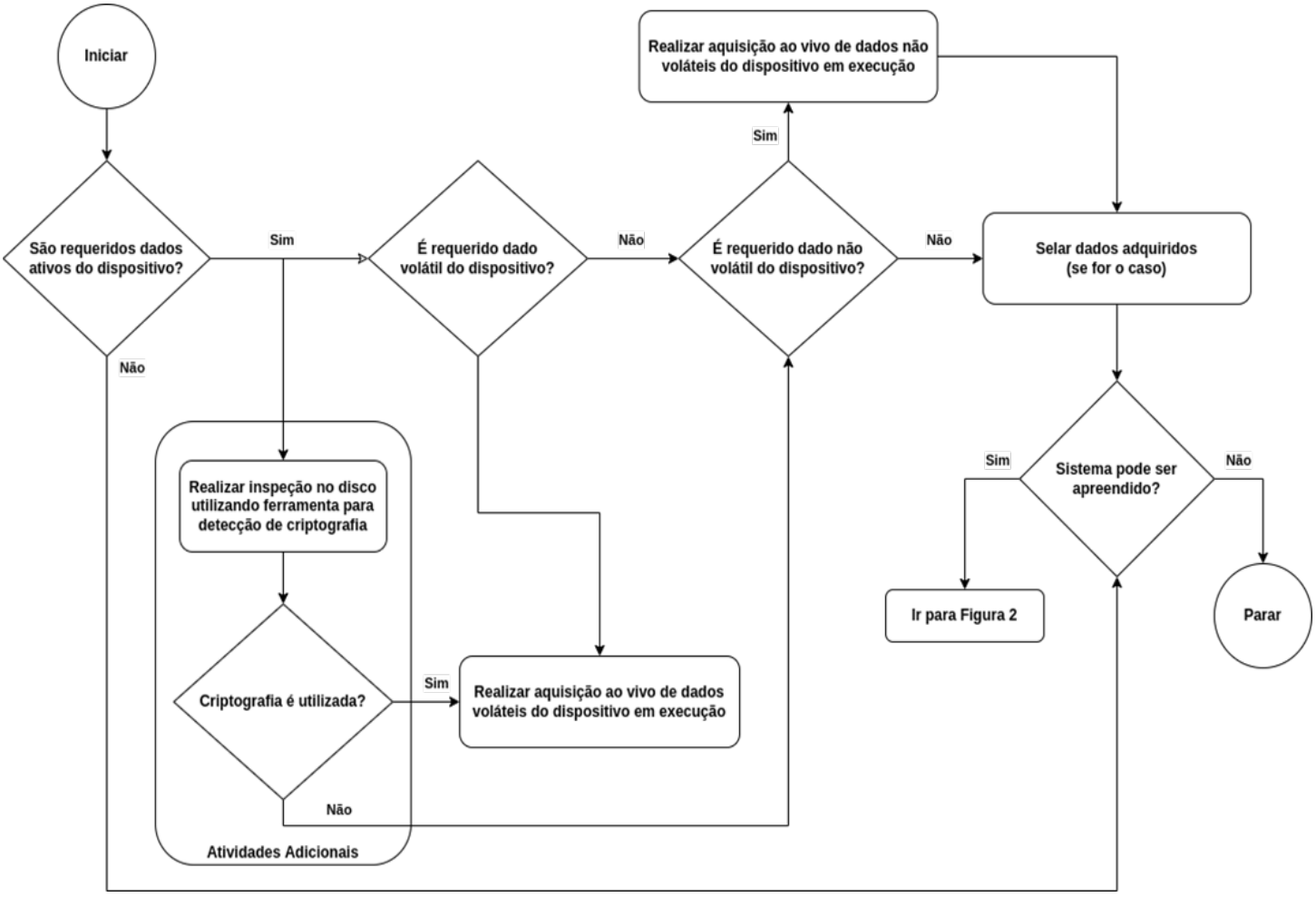
1. Possibilidade de o dispositivo digital desligar, ou de o sistema ligado entrar em modo de proteção de tela ou bloqueio automático;

2. Realização da aquisição inicial dos dados voláteis, como armazenados em memória RAM, processos em execução, conexões de rede e configurações de data e tempo;

3. Possibilidade de a aquisição ser realizada de modo presencial ou remoto;

4. Possibilidade de uso de ferramenta para detecção de criptografia.

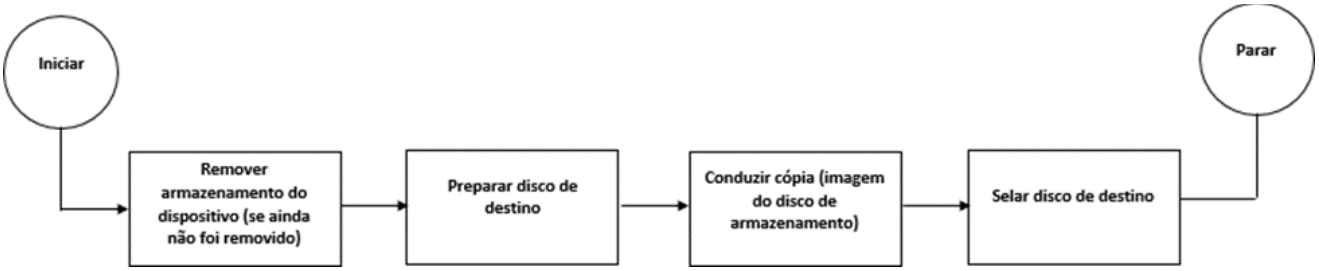
Abaixo segue o fluxo para aquisição de evidência digital em dispositivos ligados:



Antes de iniciar o processo de aquisição de dispositivos desligados, o DES deve se certificar que estão efetivamente desligados, e não em modo de espera.

Para o processo de aquisição de evidência digital em dispositivos desligados, o DES deve remover a mídia de armazenamento (por exemplo, disco rígido) do dispositivo e documentar todos os detalhes, como modelo, fabricação, número de série e tamanho.

Abaixo segue o fluxo para aquisição de evidência digital em dispositivos desligados:



O DES pode optar pela aquisição parcial da evidência digital, quando:

● O sistema de armazenamento é muito grande para ser adquirido - por exemplo, servidor de banco de dados;

● O sistema é crucial para os negócios da DMS LOGISTICS e não pode ser desligado; ● Somente dados selecionados podem conter evidências digitais;

● Em razão de ordem judicial que limita o escopo da aquisição.

Quando o DES optar pela aquisição parcial, todas as pastas, dados e arquivos relevantes devem ser identificados.

Em alguns casos, os dispositivos podem estar conectados a mais de uma rede física ou lógica. Assim, antes de desconectar o dispositivo da rede, o DES deve adquirir os dados relacionados à conexão - por exemplo, configuração de IP e tabelas de roteamento.

Para dispositivos em rede que precisam estar constantemente ligados, o DES deve impedir que interaja com rede de rádio sem fio, por meio de métodos de isolamento.

Para o processo de aquisição de dispositivos digitais em rede, o DES deve:

● Utilizar uma área de trabalho protegida;

● Utilizar um cartão SIM ou USIM que simule a identidade do dispositivo original e previna acesso à rede de trabalho pelo dispositivo, sempre que necessário;

● Adquirir a evidência digital, antes de remover a bateria.

● Quando não for possível que os dispositivos digitais sejam desligados devido à sua criticidade, pois, caso sejam interrompidos, podem afetar a continuidade das atividades da DMS LOGISTICS.

LOGISTICS, o Colaborador Especialista em Prova Digital (DES) deve realizar a aquisição imediata da evidência digital ou parcial, conforme itens 17 e 19.

Ao coletar ou adquirir uma mídia de armazenamento digital removível, o Colaborador Especialista em Prova Digital (DES) deve:

● Documentar a sua localização (por exemplo: bandejas de entrada de CD/DVD ou porta USB), fabricante, marca, modelo e número de série;

● Rotular de modo que os rótulos não sejam inseridos diretamente sobre as partes mecânicas da mídia, nem oculte informações importantes, como o número de série, da peça ou modelo;

● Estar atento à capacidade máxima de retenção da mídia digital.

21. PRESERVAÇÃO DAS PROVAS DIGITAIS

As evidências digitais e os dispositivos que as contenham devem ser armazenados em local seguro e com acesso restrito somente aos Investigadores/DES e aos colaboradores responsáveis pela sua custódia, a fim de manter a integridade e a confiabilidade das evidências.

O Investigador Líder/DES é responsável pelo registro da cadeia de custódia da evidência e pelos dispositivos até o seu descarte ou reutilização. Ele deve:

1. Utilizar uma função de verificação (hash), a fim de evidenciar que os dados copiados são equivalentes aos originais;

2. Rotular a evidência digital e os dispositivos;

3. Checar, periodicamente, os dispositivos ligados a bateria, para que tenham energia suficiente;

4. Acondicionar adequadamente os dispositivos, a fim de prevenir danos oriundos de choques, vibrações, calor, umidade e exposição a radiofreqüência;

5. Armazenar a evidência digital em mídia formatada ou nova;

6. Armazenar as mídias de armazenamento magnético em embalagem inerte magneticamente, antiestática e livre de partículas;7. Utilizar luvas livres de partículas durante o acondicionamento da evidência;

8. Proteger os dispositivos da influência de fontes eletromagnéticas.

22. TRANSPORTE DA PROVA DIGITAL

A evidência digital deve:

1. Preferencialmente, ser transportada somente pelo DES, não devendo ser deixada desacompanhada em nenhum momento;

2. Ser criptografada, caso seja necessário;

3. Ser acondicionada em local apropriado e seguro, para prevenir danificações, umidade e temperaturas inadequadas.

Todo o processo de transporte, inclusive o responsável pela realização, deve estar documentado na cadeia de custódia.

23. DOCUMENTAÇÃO

Toda atividade realizada durante o processo de identificação, coleta, aquisição, transporte e preservação da evidência digital deve ser documentada pelo DES, identificando, inclusive:

1. Data e hora dos dispositivos que estiverem ligados, comparando com a fonte de tempo estabelecida pela DMS LOGISTICS;

2. Dados visíveis nas telas no dispositivo digital, sistemas ativos e documentos abertos, por exemplo;

3. Dados dos dispositivos, como número de série, marca, modelo e fabricação;

4. Decisões tomadas e ações executadas;

5. Manuseios realizados.

Deve-se utilizar uma fonte de tempo única e documentar o tempo de cada ação.

24. ANÁLISE DE DADOS

Uma vez extraída a informação relevante, o analista deve estudar e analisar os dados para desenhar conclusões dela.

Deve ser usada uma abordagem metódica para alcançar conclusões com base nos dados disponíveis ou determinar que nenhuma conclusão ainda pode ser tirada.

A análise deve incluir a identificação de pessoas, lugares, itens e eventos, e determinar como esses elementos são relacionados para que se possa chegar a uma conclusão. Muitas vezes, esse esforço inclui dados correlacionados entre várias fontes. Por exemplo, um log do sistema de detecção de intrusão de rede (IDS) pode vincular um evento a um host, os logs de auditoria do host podem vincular o evento a uma conta de usuário específica e o log de IDS do host pode indicar quais ações esse usuário realizou. Ferramentas como registro centralizado e gerenciamento de eventos de segurança o software pode facilitar esse processo reunindo e correlacionando automaticamente os dados. Comparando características do sistema para linhas de base conhecidas podem identificar vários tipos de alterações feitas no sistema.

Se forem necessárias evidências para ações disciplinares legais ou internas, os analistas devem documentar cuidadosamente as descobertas e todas as etapas tomadas.

25. REPORT DA INVESTIGAÇÃO

A fase final da investigação forense é o relatório, onde se encontram os processos de preparação e apresentação das informações resultantes da fase de análise. Os resultados e as metodologias utilizados são descritos no relatório, incluindo os seguintes:

Explicações alternativas. No momento em que a informação relativa a um evento estiver

incompleta, pode não ser possível chegar a uma explicação definitiva do que ocorreu. Quando um
O evento possui duas ou mais explicações plausíveis, cada uma deve receber a devida consideração no processo do relatório. Os analistas responsáveis devem usar uma abordagem metódica, na tentativa de provar ou refutar cada possível explicação que for proposta. Algumas metodologias de processo forense têm uma fase de análise separada após a fase de exame. Por uma questão de simplicidade, esta publicação apresenta a análise como parte da fase de exame. Normalmente, um analista examina os dados e executa análise desses dados e, em seguida, realiza exames e análises adicionais com base nos resultados da análise inicial.

Consideração do Público. Conhecer o público para o qual os dados ou informações serão mostrados é importante. Um incidente que exige o envolvimento da aplicação da lei, como a LGPD, por exemplo, requer relatórios altamente detalhados de todas as informações coletadas, podendo também exigir cópias de todos os dados probatórios obtidos. Um administrador do sistema pode querer ver o tráfego de rede e estatísticas relacionadas em grande detalhe. A alta administração pode simplesmente querer uma visão geral de alto nível do que aconteceu, através de uma representação visual simplificada, relatando como o ataque ocorreu e o que deve ser feito para evitar incidentes semelhantes.

Informações acionáveis. O relatório também inclui a identificação de informações acionáveis, obtidas a partir de dados que podem permitir que um analista colete novas fontes de informação. Por exemplo, uma lista de contatos pode ser desenvolvida a partir dos dados que podem levar a informações adicionais sobre um incidente ou crime. Além disso, podem ser obtidas informações que podem prevenir eventos futuros, como uma backdoor em um sistema que pode ser usado para ataques futuros, um crime que está sendo planejado, um worm programado para começar a se espalhar em um determinado momento, ou uma vulnerabilidade que pode ser explorada.

Documentação. Toda atividade realizada durante o processo de identificação, coleta, aquisição, transporte e preservação da evidência digital deve ser documentada pelo analista, identificando,

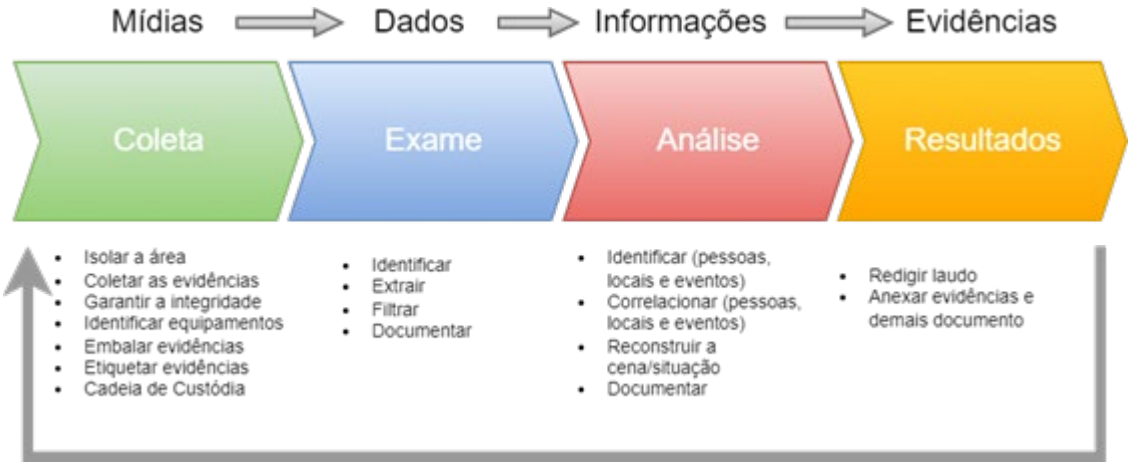
inclusive a data e hora dos dispositivos que estiverem ligados, comparando com a fonte de tempo estabelecida pela DMS LOGISTICS, os dados visíveis nas telas no dispositivo digital, sistemas ativos e documentos abertos, por exemplo, os dados dos dispositivos, como

número de série, marca, modelo e fabricação, as decisões tomadas e ações executadas e os manuseios e procedimentos realizados. O analista deve utilizar uma fonte de tempo única e documentar o tempo de cada ação.

O relatório deve conter os fatos que podem ser provados pelas provas coletadas e examinadas. Caso os dados não forneçam uma resposta clara, deve-se destacar que as

evidências não são conclusivas. O investigador poderá descrever as hipóteses plausíveis, destacando, no entanto, que essas hipóteses não podem ser corroboradas pelas evidências.

Na conclusão, se possível no caso concreto, devem ser apresentadas recomendações de melhorias.



26. LIÇÕES APRENDIDAS

Depois da apresentação do relatório para o CISO, o resultado da investigação deve ser discutido entre a Alta Administração da DMS LOGISTICS, o CISO, o Gestor de Segurança da Informação e a Equipe de Segurança da Informação.

Eles deverão verificar os processos de melhoria para evitar novas violações, avaliar mudanças nas políticas da empresa, revisão de procedimentos ou desempenho das ferramentas,

avaliando a substituição, contratação de novas tecnologias ou permanecendo na mesma situação, a depender de cada situação.

As lições aprendidas e a conclusão do processo deverão ser registradas e armazenadas em documento próprio.

27. CADEIA DE CUSTÓDIA

A cadeia de custódia tem como função promover a integridade da prova, e a possibilidade de rastrear vestígios associados ao ato criminoso, como forma de garantir e preservar a confiabilidade e transparência do processo de investigação do crime. A cadeia de custódia contribui para manter e documentar a história cronológica da evidência, para rastrear a posse e o manuseio da amostra, a partir do preparo do recipiente coletor, da coleta, do transporte até o ambiente controlado, do recebimento, da análise e do armazenamento. Inclui toda a sequência de posse.

Para garantir que a cadeia de custódia seja a mais autêntica possível, uma série de etapas deve ser seguida. É importante notar que, quanto mais informações um perito forense obtém sobre as provas em mãos, mais autêntica é a cadeia de custódia criada. Por isso, é importante obter informações do administrador sobre as evidências: por exemplo, o log administrativo, informações de data e arquivo e quem acessou os arquivos.

A cadeia de custódia deve registrar:

1. O local de coleta do dispositivo e dados;

2. Responsável pela coleta ou aquisição dos dados;

3. Detalhes do dispositivo coletado, ou detalhes dos dados que foram alvo de aquisição; 4. Detalhes dos dados adquiridos (duplicações);

5. Metodologia utilizada;

6. Ferramentas utilizadas;

7. Verificação da integridade das imagens (hash);

8. O custodiante responsável pela evidência;

9. Quem teve acesso, quando, onde e por qual motivo.

O registro da cadeia de custódia e a evidência digital devem ser mantidos enquanto for necessário para sua utilização em processos judiciais, administrativos e disciplinares na Deve-se seguir o procedimento abaixo, montado de acordo com a cadeia de custódia para evidências eletrônicas:

1. Salve os materiais originais: Sempre trabalhar em cópias da evidência digital em oposição ao original. Isso garante que seja possível comparar seus produtos de trabalho com o original preservado sem modificações.

2. Tire fotos de provas físicas: Fotos de provas físicas (eletrônicas) estabelecem a cadeia de custódia e a tornam mais autêntica.

3. Faça capturas de tela do conteúdo de evidência digital: nos casos em que a evidência é intangível, fazer capturas de tela é uma maneira eficaz de estabelecer a cadeia de custódia.

4. Data, hora e qualquer outra informação de recebimento do documento. Registrar os carimbos de data e hora de quem teve a evidência permite que os investigadores construam uma linha do tempo confiável de onde a evidência estava antes de ser obtida. No caso de haver um buraco na linha do tempo, uma investigação mais aprofundada pode ser necessária.

5. Injete um clone bit a bit de conteúdo de evidência digital nos computadores forenses. Isso garante que obtenhamos uma duplicata completa da evidência digital em questão.

6. Execute uma análise de teste de hash para autenticar ainda mais o clone de trabalho. A execução de um teste de hash garante que os dados obtidos do procedimento de cópia bit a bit anterior não estejam corrompidos e reflitam a verdadeira natureza da evidência original. Se este não for o caso, então a análise forense pode ser falha e pode resultar em problemas, tornando a cópia não autêntica.

7. Análise de acessos. A análise deve trazer informações de quem teve acesso, quando, onde e por qual motivo, assim, utilizando uma metodologia 5W2H 's para descrever cronologicamente a coleta de provas para a investigação.

O procedimento da cadeia de custódia pode ser diferente, dependendo da jurisdição em que reside a prova; no entanto, as etapas são basicamente idênticas às descritas acima.

28. DISPOSIÇÕES FINAIS

Todos os colaboradores envolvidos no manuseio da evidência digital e da investigação forense devem manter a confidencialidade do processo e do conteúdo.

Qualquer atividade que desrespeite as disposições estabelecidas nas Políticas da DMS LOGISTICS ou na legislação brasileira será considerada uma violação e tratada a fim de apurar as responsabilidades dos envolvidos, visando aplicação de sanções cabíveis previstas em cláusulas contratuais e na legislação vigente.

As violações, mesmo que por mera omissão, negligência, imprudência ou tentativa não consumada de violação às Políticas da DMS LOGISTICS, bem como demais normas e procedimentos, serão passíveis de medidas disciplinares.

Caso seja constatada violação às leis brasileiras, sejam elas penais, civis ou administrativas, as provas, evidências, dispositivos, documentos e relatórios obtidos na investigação forense poderão, se necessário, ser encaminhadas às autoridades de segurança ou judiciais. O mesmo pode ocorrer caso as informações obtidas pela investigação forense sejam requisitadas pelo Poder Judiciário.

29. IMPLEMENTAÇÃO E ATUALIZAÇÃO

A Política de Investigação Forense da DMS LOGISTICS deve ser atualizada sempre que necessário ou em um intervalo não superior a 01 (um) ano.

30. HISTÓRICO DE REVISÃO

Revisão	Data	Descrição
00	09/02/2023	Criação do documento.
01	27/02/2023	Revisão e padronização de todo o documento.

31. APROVAÇÃO E CLASSIFICAÇÃO DA INFORMAÇÃO

Elaborado por:	CyberSecurity Team	
Revisado por:	Leonardo Sabbadim	
Aprovador por:	Victor Gonzaga	
Nível de Confidencialidade:	**X**	**Informação Pública**
		Informação Interna
		Informação Confidencial
		Informação Sigilosa

NUNCA COLOCAMOS EM RISCO A QUALIDADE E NEM A ÉTICA NOS NEGÓCIOS

WE NEVER COMPROMISE ON QUALITY AND BUSINESS ETHICS

WWW.DMSLOG.COM